2022

The National Money Laundering, Terrorist Financing, and Proliferation Financing Risk Assessment 2022-2023

The United Republic of Tanzania

Ministry of Finance

United Republic of Tanzania

Ministry of Finance and Planning

THE NATIONAL MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING RISK ASSESSMENT 2022/2023

REVISED, JUNE, 2022

Contents

EXECUTIVE SUMMARY

This is a revised publication of the National Money Laundering Risk Assessment (NMLRA) since the first publication of NRA in 2019. The National Anti-Money Laundering Multi-Disciplinary Committee (National Committee/NAMCD) as the coordinating authority empowered by the Anti-Money Laundering Act (Cap. 423) and the Anti-Money Laundering and Proceeds of Crime Act No: 10 of 2009 of Zanzibar, is publishing a revised NRA taking into account COVID-19 related crimes, legislative changes and an increased cybercrime globally.

The NAMDC takes cognizance of the fact that money laundering is inevitable in all proceeds-generating crimes in order to conceal the underlying crime. As a result of this inevitability, markets and the broader financial system distortion occur. As a member of global community, the United Republic remains vulnerable to generation of all forms proceeds of crimes because of the existence of profit generating businesses as well as its position as an outlet to more than six landlocked jurisdictions (Uganda, Rwanda, Zambia, DRC Congo, Malawi, and Burundi). Criminals and money launderers continue to use a wide variety of methods and techniques, including traditional ones, to place, move, and attempt to conceal illicit proceeds. These range from the use of ill-gotten funds from, crimes such as corruption, tax evasion, to the purchase of properties such as land or expensive motor vehicles and other high-value goods, or establishing trading companies or other legal arrangements. Although the ever-evolving world of virtual assets and related service providers has not established roots in the United Republic of Tanzania, some rudimentary transactions are noted from the cash transactions reports and electronic

wire transfers linked to international virtual assets platforms or trading facilities.

The NAMDC particular concern is the prevalence of fraudulent activities involving solicitation of funds and other forms of cyber scams. Drug trafficking, cybercrime, human trafficking, smuggling, and corruption continue to exists in URT and generate significant volumes of illicit proceeds within the financial sector.

Although NAMDC takes cognizance of the COVID-19 pandemic related crimes elsewhere, there were no such incidences of criminals earning money by exploiting government-led economic support programs during the pandemic. The NAMDC takes note of pandemic leading to the increase in fraud risk for online financial services and general commerce, resulting in a dramatic spike in the number of stimuli, healthcare, bank, elder, and government fraud schemes and scams. In other countries, cybercriminals exploited the COVID-19 pandemic through phishing schemes, exploitation of remote applications, ransomware, and business email compromise (BEC) fraud.

Banking sectors and other financial service sector including the capital markets intermediaries and insurance companies demonstrate adequate anti-money laundering (AML) programs and compliance. However, almost of all DNFBPs demonstrate deficiencies while their institutions continue to be a money laundering vulnerability.

Key weaknesses within the URT AML/CFT/CPF regime include inadequate supervision of the DNFBPs, cash economy, inadequate control of physical

cash transfers, lack of timely access to beneficial ownership information of legal entities and lack of transparency in real estate transactions. There are reasons to believe that misuse of legal entities and arrangements, including limited liability companies and other corporate vehicles, trusts, partnerships, and the use of nominees, are tools for facilitating money laundering in URT especially when coupled with corruption scandals involving public servants and politically exposed persons linked with companies, professional entities or NGOs.

The objective of the 2022/2023 NRAs revision is to inform the understanding of the public and private sector stakeholders on the ML/TF/PF risks at the National level, the understanding of the risk mitigation strategies to counter these vices and possibly to inform the policy decisions by the governments of the United Republic of Tanzania and the Revolutionary Government of Zanzibar. The 2022/2023 NRA takes into consideration new areas or sectors that were not identified, analyzed or fully addressed in previous NRA. These areas include legal persons and legal arrangement, NPO sector and Terrorist Financing and Proliferation Financing Risk Assessments.

This risk assessment serves as the foundation of the 2022/2023 to 2026/2027 National AML/CF/CFP Strategy that provides a detailed roadmap of the actions that the URT will take to further strengthen our AML/CFT regime and address the long-standing vulnerabilities. Once implemented, the said actions will make the URT safer and be in a better position to identify and disrupt illicit finance. To achieve these goals, both governments of the United Republic of Tanzania and the Revolutionary Government of Zanzibar must work proactively together with public authorities, the private sector, and development partners. This assessment sets out our latest

understanding of ML/TF/PF risks, including how they have changed since the 2016 NRA. It will inform all of our continuing work to prevent money launderers from moving money through the URT.

PART I
INTRODUCTION

1.0 Background

This NRA identifies the most significant money laundering threats, vulnerabilities, and risks faced by the URT. It is based on a review of public sector analysis, enforcement actions, and guidance, as well as interviews with LEAs, intelligence analysts and AML/CFT/CPF private sector stakeholders. The NRA uses all available information to identify the current money laundering, terrorist financing and proliferation financing environment within the URT. Relevant competent authorities, agencies, bureaus, the judiciary of Tanzania, the Ministry of Home Affairs as well as regulatory agencies, participated in the development of this risk assessment. Data collected are current as of December 31, 2020.

The URT continue to be vulnerable to all forms of illicit finance because of prevalence of cash as the payment system that leave no trail to the movement of illicit funding making it difficult for tracing and confiscation. The sea port exit route for neighboring landlocked countries supporting global trade is also a vulnerability that is used by criminal for money laundering. This NRA incorporates published and unpublished materials and the analysis, insights, and observations of stakeholders who participated in its development. In drafting this assessment, the NAMDC consulted with staff from the following offices, PCCB, ZAECA, MOHA, MOFP, Police Force, DCEA, ZDCEA who also reviewed this report.

The many face-to-face meetings with operational agencies were held in Dar es Salaam when seeking input, the revision comprised information after 2019 when the onsite Mutual Evaluations exercise of URT was conducted.

This is because the period prior to 2019 was considered in the MER and appropriate recommendations were made. Post 2019 is relevant because it comprises new developments. However, as in the previous 2016 NRA, the 2022/23 NRA relies on open-source reports and the use of publicly available documentation and reports of various law enforcement agencies. In addition, this assessment includes feedback received directly from several stakeholders which provided additional insights.

1.2 Methodology

The terminology and methodology of this NRA are based in part on the guidance of the Financial Action Task Force (FATF), the international standard-setting body for AML/CFT/CPF measures. The following concepts are used in this risk assessment:

Threats: These are the predicate crimes that are associated with money laundering. The environment in which predicate offenses are committed and the proceeds of crime are generated is relevant to understanding why, in some cases, specific crimes are associated with specific money laundering methods.

Vulnerabilities: these are what facilitate or create the opportunity for money laundering. They may relate to a specific financial sector or product or a weakness in law, regulation, supervision, or enforcement.

Consequences: these include harms or costs inflicted upon citizens and the effect on the economy, which provide further context on the nature of the threats.

Risk: Risk is a function of threat, vulnerability, and consequence. It represents an overall assessment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement.

PART II
THREATS

2.0 Background

Money laundering threats are the predicate crimes that generate illicit proceeds for laundering. This section discusses the crimes that generate proceeds that are thereafter laundered through the financial system. During the period under review the assessment identifies the most prevalent money laundering threats to the URT and highlight the emerging threats that were not identified or fully addressed in previous national risk assessments. The findings related to money laundering threats within this risk assessment align with the 2022/2023 – 2026/2027 National AML/CFTCPF Strategy as mitigation measure.

This Part focuses on the understanding of the threat environment which is essential to understanding of the vulnerabilities that create opportunities for laundering illicit proceeds. The part relies on discussions with law enforcement agencies and cites specific enforcement actions in order to officially establish the magnitude and trends of the identified threats. The discussion of each threat highlights their consequences, and the effects on the economy.

2.1 FINACIAL FRAUD

Fraud related crimes continues to be the largest driver of money laundering activity in terms of the scope and magnitude of illicit proceeds, generating substantial amounts of funds. Some individual investment fraud or Ponzi schemes continue to be established and operate to generate criminal proceeds.

Examples:

Mr Kuku Scheme:

This is a case involving a person fondly known as Mr Kuku who appeared before the Resident Magistrate's Court in Dar es Salaam charged with seven counts of conducting and managing pyramid scheme, money laundering and accepting deposits from the general public without license amounting to TZS 17billion/- (USD7.3 million). Between January 2018 and May 2020 at various places within the city of Dar es Salaam, the accused conducted and managed a pyramid scheme by collecting money from the public. The accused solicited subscription from members of the public on the promise that the funds would be invested in poultry farming project in return investors would receive a 70 per cent interest of their initial capital invested for four months. According to the prosecution, the person in the alleged investment would further get another 90 per cent of the initial capital for the money invested for six months. The accused person directly engaged in transactions involving property worth TZS 6,477,297,614/83 (USD 2.8 Million) by withdrawing the sum from a bank account held at one commercial bank in the alias name "Mr. Kuku". Between January 17 and March 30, 2020 accused person was able to conduct transactions involving USD 629,249,576/36 and was able to make withdraws from the bank scheme account and depositing an estimated amount of USD 254,000 in his own personal account.

Masterlife Scheme in Zanzibar

In April, 2021, the Zanzibar President Dr Hussein Mwinyi reaffirmed the Zanzibar government's resolve to thoroughly investigate Masterlife Microfinance operations and recover all the money that the pyramid

scheme swindled from Zanzibaris. More than 10,300 people, including government officials invested in the scam. Master Life's operation in Zanzibar was suspended in February 2021 after the government questioned its financial business credibility and the government of Zanzibar arrested and prosecuted the company's executives and sold property owned by the company. The funds invested by subscribers was not invested in any legitimate business but was used to pay the people operating the scheme as well as those who invested earlier in the scheme. At the time of the suspension, more than TZS 12.32 billion was in the hands of the company. Eight in ten of the company's investors (81.2%) were low-income people who invested between TZS. 100,000 and TZS. 5 million, while 12.09 percent (1247) of the investors deposited between TZS 5.1million and TZS 10 million. Those who invested TZS.10.1million to TZS 20million were 523 or 5.07 percent, 146 or 1.4 percent invested TZS 20.2million to TZS 40million, TZS 40.5million to TZS 60million were invested by 11 people while two people invested TZS 65million and TZS 73.5million. Master Life was offering a 100 percent profit on every savings but the profit dropped to 30 percent. Investors were offered a 10 per cent interest, by purchasing food and other goods from the organizers. The company operated the scheme was holding a certificate of Registration as a foreign company issued by the Mainland's Business Registration and Licensing Agency (BRELA) and crossed over to Zanzibar where it was operating as a microfinance institution. The company main business in the registration records was livestock and animal feed manufacturer.

Peertech Company a fraud

In March 2022, nine people were arraigned at Resident Magistrate's Court, Dar es Salaam. The accused persons were Peertech Company Operating Director, the CEO of the company, the Finance Manager, Operations Manager, and Internal Auditor of the company. They were charged for committing the offenses between December 4, 2018 and December 31,2020 by colluding with NBC Bank official to collectively lead a criminal gang with the aim of committing fraud and obtaining TZS 4,786,800,000 from NBC Bank. On February 6, 2019 the defendants collectively and with the intent to commit fraud forged false documents showing 60 people were beneficiaries and employees of Peertech Company. On February 6, 2019, the defendants jointly submitted to NBC bank a false document showing the 60 people named in the document as employees of the company and credit beneficiaries when they knew it was not true. On August 30, 2019 the defendants collectively produced false documents showing the 11 people named in the agreement were the beneficiaries and employees of the company when they knew it was not true. On February 30,2019 the defendants submitted the false document to NBC bank showing that 11 people are employees which was not true. On February 13, 2020 the defendants forged false documents showing that 20 people were loan beneficiaries and that they were employees of the Peertech company and submitted the false document to NBC bank. On February 13,2020 the accused filed false documents to show that the company's shareholders had passed a resolution that 20 people had been identified at NBC bank as permanent employees and on December 4, 2018 and December 31,2020, they fraudulently obtained TZS 4,786,800,000 by submitting false

documents showing that 78 people were permanent employees of Peertech and that they were guaranteed to take out a loan through the company's contract.

In 2018 to 2020, using a list of ghost workers, Peertech Company entered into agreements with NBC, ABC and ABSA Banks. in Dar Es Salaam, and was able to obtain TZS 8 billion through fraudulent falsification of list of eligible employees for loans guaranteed by the company. In order for the suspects to achieve their evil intentions, they created and forged contracts, salary slips as well as work IDs and submitted the documents to the banks.
Similarly, in order to secure access to the forged loans, Peertech Company submitted forged documents to NMB, CRDB, DT Bank and all BOAs in Dar es Salaam.

Fraud is a broad criminal activity that can be committed in many ways or methods. All in all, financial fraud harm individuals, distorts national security, and undermines public confidence in the financial sector. Fraud also has the capacity to disrupt economic activity and put legitimate businesses at a distinct competitive disadvantage.

There is generally very low prevalence in URT of Financial frauds experienced in other jurisdictions and reported FATF or FSRBs typology study reports such as the exploitation of data, such as personal identifiable information (PII) the hacking, or compromising, as the most common methods fraudsters, launderers, and other criminals use to set up bank accounts and conceal fraudulent activity; large organized fraud groups

using vast money mule [1] networks as third-party money laundering mechanisms to launder illicit proceeds from fraud and other financial crimes (e.g., romance scams, employment scams, work-from-home scams); online scams designed to defraud victims into sending money to bank accounts, debit cards, and virtual wallets controlled by criminals; COVID-19-related Fraud and Scams such as exploiting stimulus measures by or vaccine fraud, fake cures, and fraudulent vaccine cards or generally the use of synthetic (identity fraud which is the use of a combination of real and fake PII to fabricate a person or entity in order to commit a dishonest act for personal or financial gain).

2.2 FINANCIAL CRIMES

According to the 2019/2020 statistics reports from the Police Force, there was a declining trend of offence related to illegal acquisition of property. This group of offences includes robberies, burglary, theft, arson and financial crime. In the period of January to December, 2020 a total of 24,961 offenses were reported compared to 28,853 offenses in the same period in 2019. This is a decrease of 3,892 offenses equivalent to 13.5 percent. Table 1 below indicate the total number of this group of offences reported to the police.

TABLE 1: Offences Related To Illegal Acquisition Of Property

Offence	2019	2020	Difference	Change (percentage)
Possession of fake notes	293	78	-215	-73.4
Bank robberies	10	1	100.	0
Theft in Public bodies	87	50	-37	-42.5

[1] A money mule is someone who, either intentionally or unintentionally, transfers or moves illegally acquired money on behalf of someone else.

Theft in Cooperatives societies	11	4	-7	-63.6
Theft in Local Government	21	6	-15	-71.4
Theft in central government	24	23	-1	-4.2
Theft in political parties	0	0	0	0
Forgery	781	744	-37	-4.7
Total	**1,218**	**905**	**-313**	**-25.**

Source: Tanzania Police Force

2.3 HEALTHCARE FRAUD

Although the majority of healthcare providers are honest and ethical, fraud and irregular practices do occur. Not only does this occur amongst doctors and pharmacists or at hospitals and clinics, but also amongst policyholders. Unethical behavior or action that fall outside of what is considered morally right are prevalent. This includes deceiving others for one's own benefit or financial gain. The following are indicators of unethical behavior which constitute healthcare fraud in Tanzania:

- Using someone else's policyholder card or letting someone else use your card;
- A provider supplying non-medical services (selling nappies) and claiming for these costs;
- Submitting false information on claim forms;
- a provider claiming for services not rendered. These are translating to theft, fraud, bribery and corruption in the health sector caused by- Abuse by policyholders and healthcare providers; Unethical and/or dishonest behavior by healthcare employees; unlawful, irregular or unethical conduct; Claims fraud; Over-servicing by providers; collusion between members and providers (agreeing with doctors or

service provider to send in a false claim and then sharing the money once the claim is paid).

In August 2021, the NHIF reported that the fund received TZS 600 billion/- (USD 259.7 Million.) worth of claims but after a thorough scrutiny paid only 477 billion/- (USD 206.4 million) in 2020. The amount paid was 77 per cent of the total claims. According to the Controller and Auditor General (CAG) report for the period 2020-2021, there were 7,556 claims worth TZS 69.1 million ($29,785) that names of the beneficiaries did not correspond with that of the card holder. There were also some 444 members who received full blood picture examination more than once on the same day. The CAG reported that the Tanzania's National Health Insurance Fund (NHIF)paid hospital bills for men to undergo caesarean and normal delivery. 731 men were reportedly part of the fraud. Further the CAG reviewed and identified that false claims were submitted by health facilities and were paid TZS14,409,200 ($6,211) and that 56 claims showed that men received caesarean operation or normal delivery service. In addition, there were some 444 members who received full blood picture examination more than once on the same day some even more than 30 times at the same health facility. There were members who received spectacles more than once yet the law only allows for such a service once in a year.

As healthcare fraud schemes can be complex and have involved complicit doctors, pharmacists, and other medical professionals, the money flows can mimic legitimate transactions from insurers to healthcare providers. In some cases, complicit healthcare providers and other companies in the healthcare field have incentivized patients to purchase their services or products by illegally offering to pay some benefits.

2.4 DRUGS TRAFFICKING

Drug trafficking continues to pose a threat to public health in the URT and continuous to generates significant proceeds for the criminal organizations that supply the URT and global markets. Tanzania-based trafficking organizations and courier networks operate globally and play a prominent role in the southwest Asian heroin trade, using Dar es Salaam port as the launchpad to control the trade in East Africa. The countries' location as exit to six landlocked countries, porous borders and persistent corruption present challenges to drug interdiction[2].

International drug trafficking entities and courier networks transit through Tanzania to smuggle heroin from southwest Asia. Traffickers transport heroin via small vessels to Zanzibar and mainland Tanzania and over Tanzania's land borders with Kenya and Mozambique to destinations in Europe and North America. Porous borders and inadequate port security present considerable challenges to drug interdiction efforts.

Example:

On Oct. 24, 2017, two Iranian nationals were arrested on the Tanzanian territorial waters in the Indian Ocean by the authorities with a consignment of drugs. Nabibaksh Pribaksh Bidae, the captain of the ark, and his assistant Mohamed Hanif, were convicted of two offences of trafficking 111.02kg of heroin and 235.78 grams of cannabis resin. They were sentenced to 30 years

[2] The 2021 International Narcotics Control Strategy Report by the Bureau for International Narcotics and Law Enforcement Affairs

in jail each in Tanzania for smuggling a big consignment of illicit drugs using a wooden dhow.

As a conduit for heroin smuggling, criminals have, for years, been using loopholes and circuitous routes across East Africa to dodge authorities and import drugs from Afghanistan and other destinations as they desperately try to smuggle them to Europe. Local and international media reports suggest that heroin coming from Afghanistan has been passing through Pakistan's southwest coast, and taken by motorized wooden dhows to the east African coast.

The 2015/20 strict measures by Tanzanian government led to the arrests of dozens of smugglers in a series of raids and clandestine operations in Dar es Salaam, Kilimanjaro and Tanga, seizing hundreds of kilos of heroine. Customs officials at Dar es Salaam port have repeatedly intercepted shipping containers concealing illicit drugs.

Example:

In April 2020, the DCEA seized 300kg of heroin in Dar es Salaam and arrested a Nigerian and two Tanzanian nationals. The seizure represented one of the largest in Tanzania's history and underscored the government's commitment to the operation. Drug traffickers use financial incentives to influence politicians, law enforcement and others in positions of power.

In August 2020, the DCEA seized more than five metric tons of marijuana as a result of multiple ongoing drug investigations. In September,2020 Tanzanian police seized 51kg of heroin and arrested eight suspects.

The United Republic of Tanzania has continued to adopt drug control policies and strategies through integrated and balanced approach in response to emerging and evolving realities on the world drug problem including the links between drug trafficking and other forms of organized crime. Between June 2019 to December 2021, Tanzania experienced a surge on drug trafficking, and illegal trafficking of precursor chemicals. A total of 1100kg of heroin and 452 kg of Methamphetamine were seized by DCEA through the illicit drug trafficking of Southern Route from South East Asia.

Drugs are being trafficked using dhows of Iranians and Pakistanis. There are numerous demand reduction and harm reduction interventions in the country such as Integrated Methadone Assisted Therapy services in which 12 sites are operating with more than 10500 people with opioid use disorder attending on daily bases.

Example:

In June 2022 the DCEA reported to have seized 877.217 kilograms of heroin and cannabis in the five months through an electronic system known as "Pen Online System" they also managed to prevent 122,047 kilograms of heroin and 85 liters from entering the country. Out of 877.217kg of drugs, 174.112kg was heroin while 703.105kg was cannabis. Six suspects were involved but only one was arrested. Investigations by the Chief Government Chemist verified 163 packets of drugs were heroin, weighing a total of 174.112kg.

On 27th and 31st January 2022 Police Force in Zanzibar at Abeid Amani Karume International Airport (AAKIA), arrested two women at different

incidences accused of drug dealing, with a total of six kilograms of heroin. The suspects were a 52- and 32-years old women. One suspect hailed from Mainland Tanzania was travelling in an Ethiopian Airline plane from South Africa, with 4.36 kilograms of heroin.

Zanzibar has been frequently mentioned as the main drug gateway, transit and trafficking hub to Europe and United States of America, with the islands hosting over 10,000 out of the world's 200 million drug abusers. In addition, Zanzibar's location makes it susceptible to the heroin trade from Afghanistan and Pakistan, which are located across the Indian Ocean from the East African coast.

Zanzibar is a long-established drug-trafficking hub in the region, primarily for heroin, hashish and cocaine. Historical trade links with what is now Iran, Pakistan and India may in part be why Zanzibari traffickers were among the first people from the African continent to exploit the opportunity to traffic heroin and hashish from these areas. Most consignments are intended for onward trafficking to Europe and North America. There is also an active local market driven by tourism, particularly for cocaine, which is used by some wealthy Zanzibaris, but also for heroin, the use of which is increasing among the general Zanzibari population.

Heroin began appearing in Zanzibar in the mid-1980s, when it was consumed mostly by tourists, but also by wealthy Zanzibaris and other local users who had picked up the habit working elsewhere and had returned to the island. It was also brought by mules travelling from Iran, Pakistan, Afghanistan and India. The quality of product was high such that it was nicknamed ‘brown sugar’. In the late-1990s, the number of heroin users began to grow substantially and as Zanzibar opened up to international

tourism, the tourist-led demand for heroin increased. Local heroin uses also grew both Unguja and Pemba. To date numerous established dealers, exit who control drug sales in villages across the two islands. They also employ hustlers to sales the drugs.

2.5 CYBERCRIME

Tanzania estimated internet users reached 1,515 in January 2021. The number of internet users increased by 435 thousand (+3.0%) between 2020 and 2021. Internet penetration stood at 25.0% in January 2021 and there were 5.40 million social media users in Tanzania in January 2021. The number of social media users increased by 900 thousand (+20%) between 2020 and 2021 and that was equivalent to 8.9% of the total population in January 2021. There were 50.15 million mobile connections in January 2021 indicating an increase of 2.6 million (+5.5%) between January 2020 and January 2021.The number of mobile connections in January 2021 was equivalent to 82.7% of the total population.

The Tanzania Cybercrimes Act of 2015 was enacted by the Parliament in April 2015 criminalizing offences related to computer systems and Information Communication Technologies; provides for investigation, collection, and use of electronic evidence in Tanzania Mainland and Zanzibar and penalizes a number of cyber activities such as data espionage, publication of child pornography, publication of pornography, publication of false, deceptive, misleading or inaccurate information, production and dissemination of racist and xenophobic material, initiating transmission of or re-transmission of unsolicited messages and violation of intellectual property rights and other types of cybercrimes. This law came

after significant impacts such as financial loss, fraud and cyber bullying to the public and other stakeholders.

The official statistics about the trend of cybercrimes in Tanzania indicate that in 2020 the Police Force Cybercrime Unit continued to receive complaints citing suspected criminal activities facilitated by the internet. These mainly constitute self-reported loses. The complaints received by Cybercrime Unit are a fraction of cybercrimes occurring in Tanzania. Law enforcement and supervisory assessments, as well as reports from financial institutions, confirm the assessment that cybercrime is growing and may assume a significant share of the overall money laundering threat in Tanzania.

There is generally a low prevalence of cybercrimes in Tanzania compared with other jurisdictions where cybercriminals and malicious actors took advantage of the COVID-19 pandemic through phishing schemes and exploitation of remote applications to conduct ransomware attacks and fraud. URT take cognizance of cybercrime threats and remains vigilant on cybercriminal groups that elsewhere, they deploy malware to harvest data, which they have monetized through online marketplaces or direct exploitation.

URT also take cognizance of the fact that cybercrime presents a significant illicit finance threat and that the size, reach, speed, and accessibility of the financial system financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and foreign state actors. Further URT take cognizance of the fact that among the critical infrastructure targets, include the websites, systems, and employees' theft of customer and

commercial credentials and proprietary information to defraud institutions and their customers, and disrupting business functions.

Cybercriminals often use of remote desktop protocol endpoints and phishing campaigns to harvest credentials or otherwise gain access to a victim's computer network is noted and financial institution are urged to take note and be vigilant. Ransomware actors sharing resources, such as exploit kits or forming partnerships with other cybercriminals to enhance their effectiveness of attacks are other methods to watch for in URT. Ransomware developers selling access to their malware to affiliates in a "ransomware-as-a-service" model, and thereby decreasing the barrier to entry and level of technical expertise required to conduct ransomware attacks should also be noted. Further, ransomware actors increasingly employment of double extortion tactics, where criminals steal confidential data before encrypting it and threaten to publish the data if the victim does not pay the ransom should also be watched by AML/CFT stakeholders.

During the pandemic, in other jurisdictions, criminals required ransomware-related extortion payments to be made in virtual assets, frequently in bitcoin. Experts' analysis in those jurisdictions indicated that some ransomware actors demanded payment in anonymity-enhanced cryptocurrencies (AECs), requiring an additional fee for payment in bitcoin or only accepting payment in bitcoin after negotiation. It was also indicated that virtual wallets associated with top ransomware variants were used to send funds to virtual asset service providers (VASPs), in particular exchanges. Note should be had on the use foreign virtual asset service providers for ransomware-related deposits, which have weak or

nonexistent AML/CFT controls, before the perpetrator launders and cashes out the funds. They also avoid using the same wallet addresses and use chain hopping of mixing services and decentralized exchanges.

The NAMDC strongly discourage the payment of cyber ransom or extortion demands, which can be used to finance future attacks or other illicit activity. In some cases, the attackers may refuse to honor the payment and the victim is unable to restore data and operations. In such cases, timely victim notification to and the LEAs are encouraged.

2.6 BUSINESS EMAIL COMPROMISE

Cybercriminals in other jurisdiction have exploited the COVID-19 pandemic by using BEC schemes, where scammers can generate significant illicit proceeds when they convince those unaware members of the public to wire down payments to illegitimate accounts. In BEC schemes, criminals use compromised or spoofed accounts, often those actually or purportedly belonging to company leadership, vendors, or lawyers, to target employees with access to a company's finances to induce them to transfer funds to bank accounts thought to belong to trusted partners. During the pandemic, criminals exploited pandemic-related changes in business operations, the high demand for critical pandemic-related supplies, and remote work operations to convince victims to make payments and often made last-minute and urgent demands for a change in recipient account information and the timeline for payment.

2.7 COMPROMISE AND SALE OF FINANCIAL INFORMATION

Some cybercriminal groups develop and deploy malware to harvest and monetize financial data on an industrial scale from businesses around the world. Some groups use botnets, or networks of compromised computers that can include hundreds of devices, which they can command and control to launch attacks against a large number of computers at once to extract information, including banking passwords and login credentials. Criminals can traffic the harvested data through market places that specialize in the sale of compromised debit and credit cards, PII, financial and banking information, and other contraband. Such marketplaces may be established by other cybercriminals using turnkey online storefront design and hosting platforms.

Purchasers of harvested data may attempt to use credentials and other PII to access victims' accounts at financial institutions to conduct unauthorized financial transactions, create synthetic identifies, or commit identity theft.

2.8 PROFESSIONAL MONEY LAUNDERING

Professional services remain attractive to criminals as a means to create and operate corporate structures, invest and transfer funds to disguise their origin, and lend layers of legitimacy to their operations. The NAMDC would like to bring to the attention of AML/CFT/CPF stakeholders in URT of the use of professional money laundering organizations (PMLOs), networks, and third-party money launderers; although this is not common in Tanzania, it is worth noting since these groups are considered a threat given that they are criminal actors (money brokers). PMLOs, have been used to launder

funds on behalf of organized criminal entities operating in several countries around the world. Some of the PMLOs have been used to launder the proceeds of cybercrime or carry out several activities, including conducting money pickups of drug proceeds, transporting the cash, depositing the money into the banking system, and/ or transferring the money to different individuals or entities. PMLOs use casinos, front companies, foreign and domestic bank accounts, to launder money on behalf of transnational drug trafficking entities.

Criminal groups have offered professional money laundering services through online advertisements. For example, in 2020 and 2021 in the US, 14 members of the Infraud Organization were convicted of racketeering charges including money laundering offenses. Operating under the slogan "In Fraud We Trust," traders on international, members-only clear and darknet sites could engage in the large-scale sales of stolen identities, financial and banking information, and computer malware and post advertisements offering illegal money laundering services.

2.8 CORRUPTION AND RELATED OFFENCES

Corruption takes on many forms and is used to further various illicit behaviors. Types of corruption include grand corruption, administrative corruption, state capture, and strategic corruption.[3] Public corruption within the URT involves the corruption in the local government authorities and the central government and other public institutions. The proceeds of foreign corruption affect the URT when foreign corrupt officials seek to invest their illicit proceeds in or through the Tanzanian economy. These

crimes are generally committed for private gain and often rely on money laundering to conceal or hide the source and ownership of the illicit proceeds. Corruption prevents citizens from receiving what they are due, from social services. It can manifest as citizens, especially the wealthy, evade payments they owe, including tax obligations and other fees. Corruption is major impediment to economic fairness and growth in many countries and a detriment to good governance. The 2015 NRA identified corruption as a priority money laundering threat and that domestic corruption was prevalent.

Tanzania climbed up one place to 87 among 180 countries in a corruption perception index (CPI) of 2021, according to Transparency International. The index, which ranks 180 countries and territories by their perceived levels of public sector corruption according to experts and business people, uses a scale of 0 to 100, where 0 is highly corrupt and 100 is very clean. It relies on 13 independent data sources and uses a scale of zero to 100, where zero is highly corrupt and 100 is very clean. In the 2021, Tanzania scored 39/100, making it one of the least corrupt countries in the East African region. Tanzania is ranked the second least country in the region behind Rwanda, which occupies 52nd position with a 53/100 score. Kenya, Uganda and Burundi are ranked 128th, 144th and 169th respectively.

Both grand and petty corruption are serious problems in Tanzania despite existence of the law to prevent corruption. The major reason for corruption in URT is largely due to a weak internal control and low or non-compliance with anti-corruption laws and regulations. Corruption is prevalent in public procurement, taxation, and customs service . The existing large informal sector of 48.1% of GDP creates opportunities for corruption.

2.9 TRAFFICKING IN PERSONS AND SMUGGLING OF IMMIGRANTS

Human trafficking crimes generally involve compelling or coercing a person's labor, services, or commercial sex acts, or causing a minor to engage in commercial sex. Human trafficking does not require the crossing of an international border and is a crime distinct from the crime of human smuggling. Human smugglers engage in the crime of bringing people across international borders through deliberate evasion of immigration laws, often for financial benefit. While human trafficking and human smuggling are distinct crimes, individuals who are smuggled are vulnerable to becoming victims of human trafficking and other serious crimes. Both human trafficking and human smuggling networks pose a serious criminal threat with devastating consequences as criminal organizations value profit over human life.

2.9.1 Human Trafficking

Human trafficking is a financially motivated crime that harms the safety and security of those trafficked throughout the URT and the world. It is a misconception that human trafficking requires crossing a border. Human trafficking victims in the URT may be citizens, foreign nationals who have lawful immigration status, or individuals who are unlawfully present.

Human traffickers take advantage of poverty, conflict, natural disaster, breakdowns in the rule of law, dislocation, disruption of social support systems, and other global crises that can intensify victims' vulnerabilities to recruitment and exploitation.

Over the past five years, human traffickers in URT exploited domestic and foreign victims and traffickers exploited victims from Tanzania abroad. Traffickers often deceive family members, friends, or intermediaries into aiding traffickers in their exploitative tactics by fraudulently offering assistance with education, offering better living conditions, or securing employment in urban areas and abroad.

Sometimes the brokers enter communities to recruit and transport victims into trafficking situations. Impoverished and orphaned children from the rural interior, children with disabilities, and Burundian and Congolese refugees and migrants remain most at risk to trafficking.

Traffickers exploit girls in domestic servitude throughout the country and in sex trafficking, particularly in tourist hubs along the border with Kenya.

Women, children, internally displaced persons, and migrants have been victims of forced labor or sex trafficking, Cuban medical workers working in Tanzania have been forced to work by the Chinese and Cuban government, and Chinese nationals may have been forced to work by their employers, including Chinese state-owned enterprises. The NGO in question stated that traffickers target young girls from rural and impoverished villages, pay their parents a small fee, and coerce the girls into sex trafficking, specifically targeting business people.

Traffickers' subject children to forced labor on farms—including as cattle herders and occasionally as hunters—in gold and gemstone mines and

quarries, the informal commercial sector, and on fishing vessels operating in Tanzanian and international waters.

Some unscrupulous individuals manipulate the traditional practice of child fostering—in which poor parents entrust their children into the care of wealthier relatives or respected community members—and subject children to forced labor as domestic workers. Some women and girls travel to Zanzibar from mainland Tanzania with promises of marriage or good jobs and then are forced to work as farm laborers.

Examples:

In 2017, an NGO reported 14 Indonesian trafficking victims were identified aboard a Malaysian-flagged fishing vessel and in 2018, another NGO reported that 12 Tanzanian trafficking victims were identified aboard a Chinese-flagged fishing vessel, both in Tanzanian territorial waters.

Media reports have indicated traffickers transporting Tanzanian children with physical disabilities to Kenya and forced them to work as beggars or in massage parlors. In 2018, the Kenyan government identified 29 female Tanzanian potential victims in Kenya; the girls were to be taken to the United Arab Emirates (UAE) and to pay for their transportation fees with a kidney.

Traffickers sometimes subject Tanzanians to forced labor, including in domestic service, and sex trafficking in other African countries, the Middle East, Europe, Asia, and the United States. Traffickers and their victims transited through Zanzibar for forced domestic service in Oman and the UAE.

Ethiopian migrants and victims' transit through Tanzania en route to South Africa and Burundian victims are increasingly transiting through Dar es Salaam en route to Oman, UAE, and Kenya.

Citizens of neighboring countries may transit Tanzania before traffickers subject them to domestic servitude or sex trafficking in Kenya, South Africa, Europe, and the Middle East. Children from Burundi and Rwanda are increasingly subjected to child forced labor in Tanzania. Trafficking victims subjected to forced labor in Tabora were reportedly from rural areas of Kigoma—a region that hosts refugee camps and settlements.

Example:

In 2019, North Koreans working in Tanzania may have been forced to work by the North Korean government. According to international bodies, the North Korean government has been accused of systematically requiring forced, uncompensated labor from most of its population—including workers at state-owned enterprises or deployed overseas, women, children, and prisoners—to control its people and sustain its economy. In that regard, a significant majority of North Koreans must perform unpaid labor, often called "portrayals of loyalty" at some point in their lives.

The government of United Republic of Tanzania increased protection efforts, ensured implementation of regulations that requires police force and immigration authorities to use standardized procedures and forms for case investigation and victim identification and referral.

In 2021, 165 potential trafficking victims were identified, compared with 161 in previous year. The victims were referred all to either NGO-run shelters or government-vetted and trained host families. Of the 165 identified and referred victims, 145 were female, 20 were male, 139 children, and 26 were adults; this compares to 159 females, two males, one adult, and nine unknown identified and referred victims in 2020.

In January 2021, the government identified, referred to care, and reintegrated into their home communities 38 disabled victims exploited in forced begging in Dar es Salaam. Separately, Anti-Traffick Secretariat reported reintegrating 42 child trafficking victims with their families.

In 2020, the government finalized and launched the National Guidelines for Safe Houses. The guidelines established standards for safe houses, which could provide shelter for trafficking victims, and codified a joint plan to create and run government-operated shelters, offered guidelines for screening shelter residents for trafficking indicators, and provided for protection of human trafficking case files.

The 2008 anti-trafficking law mandated the government to provide victims with psychosocial counseling, family tracing and reunification, and temporary shelter and mandated the government to provide a central repository of funds for victim protection support and provided foreign victims legal alternatives to their removal to countries where their safety or that of their families may not be endangered. The Anti-Trafficking Fund was launched in 2020 authorizing the ATS to oversee and manage the fund.

The government repatriated two Tanzanian victims from abroad, one identified in Malaysia and the other in Iraq, in 2021 while a total of 10 total repatriations were made in 2020.

In 2021, the government in collaboration with other international organizations facilitated the return of 21 Burundian victims identified en route to the Middle East and one Mozambican girl exploited in Tanzania.

In 2021, 243 Burundian child victims were identified in Tanzanian refugee camps and were returned to Burundi. The government provided assistance to foreign victims by facilitating travel documents and providing secure passage to borders.

2.9.2 Human Smuggling

Human smuggling involves illegally transporting people, who have consented to their travel, into the URT and, potentially, the subsequent harboring of those individuals in the URT. Human smuggling is an inherently transnational crime. Moving human beings as cargo pays for transnational criminal smuggling organizations. Illegal smuggling fees can range from a few hundred dollars to over $10,000. According to immigration reports, more than 15,786 illegal immigrants were arrested in Tanzania between 2020 and 2021, mostly from the Horn of Africa and the Great Lakes Region.

Example:

In January 2022, Tanzanian Police and immigration officers in Dodoma intercepted 51 Ethiopian immigrants on their way to South Africa. The Ethiopians were hidden in a truck that was loaded with fresh tomatoes, travelling from Kilimanjaro region in northern Tanzania to the south.

Ethiopian immigrants used to enter Tanzania then travel through the coastal zone, but police road blocks have seen truck drivers use other routes.

Immigrants generally enter Tanzania with support of locals through negotiated payments of between $1,600 and $3,000 each to syndicates who facilitate the move to South Africa, Botswana and Namibia.

In 2020 1,000 illegal immigrants were arrested in Tanzania between July and October, mostly from neighboring countries and the Horn of Africa. Porous borders between Kenya and Tanzania has been identified as key entry points for Ethiopian and Somali immigrants. The borders between Kenya and Tanzania in Kilimanjaro, Arusha and Tanga regions are the most known entry for illegal immigrants, with a few sneaking through the Indian Ocean from Lamu, Mombasa then Pangani in Tanga. Namanga (Arusha), Holili and Tarakea (Kilimanjaro) and Horohoro (Tanga) have hundreds of unmanned entry points while informal ports are used by speed boats along Tanga's Indian Ocean coastline to ferry immigrants from Somalia via Mombasa.

2.10 ILLEGAL WILDLIFE TRADE

The IWT includes the trade in species that are protected and prohibited from all national or international commercial trade, and the trade in volumes of certain species of wild origin which is unsustainable and in violation of provisions set nationally or by the Convention on the International Trade of Endangered Species. By the beginning of 2020 at least 11 organized wildlife trafficking syndicates had been identified and 21 "kingpins"/perpetrators or the high-level leaders and organizers of the

illegal trade, who profit most from it were arrested including Yang Fenglan, a Chinese businesswoman known as the 'Ivory Queen'.

Previously, Tanzania suffered poaching on an "industrial scale", leading to a 60% decline in its elephant population in just the five years between 2009 and 2014. The figures, from a government census, equate to a loss of more than 60,000 elephants. The International Union for Conservative Nature (IUCN) categorized the African savanna elephant as Endangered species.

Elephant populations in Tanzania have risen from 43,000 in 2014 to 60,000 in 2019, and the number of elephants in the Serengeti Ecosystem rose from 6,087 in 2014 to 7,061 in 2020. In December 2020, the analysis of ivory seizures suggested that poaching had shifted from East Africa to Central and West Africa in the past five years.

It is estimated that 87 tons of ivory seized worldwide between 1998 and 2014 was linked to Tanzania, making the country the global hotspot for ivory poaching during those years. Between 2015 and 2019, less than five tons of seized ivory was believed to be linked to Tanzania compared to the figure for Nigeria during those years which was more than 30 tons. Today Tanzania is no longer seen as a major exit for ivory although it doesn't mean it's gone away completely. The multi-agency approach was instrumental in dealing with this problem. The traffickers exploit loopholes and weak governance, and so having multi-agency co-operation is key.

Since 2015 a total of 3,541 suspects involved in the illegal wildlife trade at different levels were identified and blacklisted. On average each commanded about 5 to 10 people, consisting of collectors, transporters and middlemen.

Arrest reports suggest that alongside Tanzanians, both Chinese and West African criminal networks are at play in the country, but that the 'leading players' are Asian criminal networks, which purchase illegal products locally and export them to Asia. As well as 14,000 pieces of ivory seized, 25 rhino horns, 29 hippo teeth and 29 "big cat" skins were also seized in five years, as well as hundreds of live animals and thousands of tons of timber.

PART III
VULNERABILITIES AND RISK

3.0 BACKGROUND

In the context of this NRA, a money laundering vulnerability is what facilitates or creates the opportunity for money laundering, terrorist financing or proliferation financing. Vulnerabilities may relate to a specific financial sector or product, or a weakness in regulation, supervision, or enforcement. They may also reflect unique circumstances in which it may be difficult to distinguish legal and illegal activity. The methods that allow for the most amount of money to be laundered quickly or with little risk of being caught present the greatest potential vulnerabilities. Residual risk is a function of threat and vulnerability and represents an overarching judgment, taking into consideration the effect of mitigating measures including regulation, supervision, and enforcement, among other things.

Money launderers, terrorist financers and proliferation financers attempt to identify and exploit the vulnerabilities, given the nature, location, and form of their illicit proceeds or the funds to finance terrorism or proliferation. Money laundering methods shift and evolve in response to opportunities and changes in financial services, regulation, and enforcement.

3.1 CASH BASED MONEY LAUNDERING VULNERABILITIES

Cash-based money laundering is still heavily characterized by the use of cash intensive businesses to disguise criminal sources of wealth, or by smuggling large amounts out of the URT. This is alongside continued abuse of legitimate URT services, such as money transmission and retail banking. The use of cash couriers and cash-intensive businesses remains a major

AML/CFT/CFP risk in Tanzania due to its ability to leave no trail and making it impossible for investigation to trace. The use of cash provides an opportunity to money launderers to deposit their illicit cash into the formal financial system. Many businesses in Tanzania are still cash-intensive businesses and therefore are extremely vulnerable to money laundering.

3.1.1 Bulk Cash Transportation/Smuggling

COVID-19, at least temporarily, changed the money laundering landscape due to a decrease in commercial air travel, shipping delays, and border restrictions. During that period, people had difficulty transporting bulk currency from the URT to other destinations. Cross Border declarations in all major border points declined drastically. It is believed that this resulted in people accumulating large amounts of funds. Although the pandemic led to a temporary decline in bulk cash transportation or smuggling, it is also believed that there is a significant continued repatriation of large volume of cash including illicit proceeds across URT border points. This is accelerated by the high frequency of the use of all major border points by neighboring countries.

An analysis of cross border cash transactions was conducted in 2020 indicated that a lot of money was transported across the border in cargo. During years 2019 and 2020 a total cash cargo export declared was more than USD 1.6 billion. The currency declaration at border points generally decreased in year 2020 due to COVID-19 pandemic impact. However, in terms of cash cargo exports, there was a decrease in cargo currency export declarations in terms of volumes and value. It is believed that people who could not travel with cash, they deposited the same in banks. New

York, England, Germany, and Kenya were leading destinations. Although the banking industry is adequately regulated, there is need to look into cash transaction to ensure that they are not abused by criminals.

3.1.2 Postal Money Orders

Money orders are negotiable financial instruments, which represent a convenient, widely accepted form of payment. They are more secure than cash, and unlike checks, money orders cannot bounce as the funds are prepaid at the time of purchase. The Tanzania Post Corporation (TPC) indicate that it continuous to provide registered mail requiring special handling be affected on its contents, which may be money order, postal order, Bank draft etc.

Six (6) approved money transfer companies/operators (MTO) operate in Tanzania (African Express Money, Money Gram, Western Union, World Remit and Terra Payment Services Limited). The existence of these companies suggests that money orders continue to be a popular form of payment utilized by the members of public in Tanzania. In this regard, money orders may also continue to be exploited by criminals. To criminals, money orders facilitate a wide variety of criminal activities ranging from fraud to narcotics trafficking to human trafficking because they offer a vehicle to convert illicit proceeds to a monetary instrument that is not inherently suspicious in nature. Furthermore, criminals may seek to launder their funds through a money courier while also remaining relatively anonymous throughout a transaction.

Money orders are purchased using cash, debit cards, and traveler's checks payable in currency of their choice. The NAMDC takes cognizance of the opportunity presented to criminals by all forms of money orders or money courier services to launder illegally obtained fund by purchasing money orders.

Postal Money orders is rated medium high given the ease of which the service provides opportunity to criminals to launder illicit obtained funds.

3.1.3 Funnel Accounts

A funnel account involves an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals. They are typically seen in a variety of complex frauds and scams and may also be used by criminals and fraud networks to get illicit cash proceeds out of the United Republic. Use of funnel accounts is evidence by STR reported and it is observed that this is a common prevalence. Cash activity occurs at financial institution branches across Tanzania by small businesses indicating likelihood of tax evasion, scams or concealment of other unlicensed businesses. Most often, owners of potential funnel accounts make cash withdrawals or transfers immediately after the deposits are made.

This is rated as Medium High

3.1.4 Cash-Intensive Businesses

The use of cash-intensive businesses is one of the oldest and most reliable methods to place and layer illicit funds. Cash intensive businesses is affected through the use of a front company. Front companies are fully functioning companies, often having a physical location, with the characteristics of a legitimate business. Experience shows that illicit proceeds have been laundered through cash-intensive businesses, such as convenience corner stores, auto repair shops, used motor vehicle dealership, gas stations, clothing companies and restaurants. In such examples, the cash deposits and subsequent activity in their bank accounts do not align with what a legitimate business would show.

Given its significance in obscuring money trail and taking cognizance of typology studies ML/TF/PF vulnerabilities in cash intensive business the NAMDC has put specific strategies in the National AML/CFT/CPF Strategy 2022/23- 2026/2027, to deal with the whole question of cash economy. In the mean while the law currently has identified all cash intensive business as reporting persons required to implement preventive measures including customer due diligence (CDD) requirements.

3.2 MISUSE OF LEGAL ENTITIES

The previous NRA 2016 did not consider the threats, vulnerabilities and risks pertaining to mis-use of legal persons and legal arrangements. Legal persons and legal **a**rrangements are corporate vehicles that are commonly misused for illicit purposes. The FATF Recommendations 24 and 25 deal with the transparency of legal persons (such as companies) and arrangements (such as trusts). The FATF also requires a better understanding by all

AML/CFT/CPF stakeholders of the associated risks of such entities under their jurisdiction. Various typologies studies suggest that shell companies, either in URT or offshore, are a common conduit for ML. The misuse of corporate bank accounts features in cases of online fraud, email/telephone scams and investment fraud. International drug cartels or entities use local bank accounts opened by stooges/mules and shell companies to dissipate drug proceeds. Local bank accounts and offshore companies as well as corporate vehicles, trusts, and nonprofit organizations have been proved to be used to hide proceeds of corruption. Complex corporate structures and trusts have also been proved to be used to conceal ownership and control of proceeds of foreign tax evasion. Almost all ML cases prosecuted in URT involve corporate accounts of legitimate businesses which have been exploited, or set up by criminals to hide beneficial ownership.

URT has formation procedures for variety of legal persons and legal arrangements including the companies, association/societies, sole proprietorships, partnerships, trusts, cooperatives, and NGOs. Legal persons and legal arrangements are commonly incorporated to carry out business or services or to open bank accounts. Legal persons and legal arrangements can be used at the layering stage in an ML/TF/PF transaction to make it difficult and time consuming to trace proceeds of crime. In cases involving the use of more advanced ML techniques, front legal persons or legal arrangements can be established to transfer crime proceeds from one jurisdiction to another under the disguise of payments resulting from legitimate business activities/services, such as imports and exports.

There is less available data on the misuse of legal persons and legal arrangements as no research has been carried out to show the magnitude of this problem. The NAMDC take cognizance of the risks as reported in FATF and FRBS typology studies and the recent international incidents such as the Panama Papers that highlighted the possible abuse of corporate structures and legal arrangements at the international level. The Panama Papers are 11.5 million leaked documents published in 2016 detailing financial and attorney–client information for more than 214,488 offshore entities. The documents contain personal financial information about wealthy individuals and public officials that had previously been kept private. While offshore business entities are legal reporters found that some shell corporations were used for illegal purposes, including fraud, tax evasion, and evading international sanctions.

3.2.1 Legal Persons and Legal Arrangements

(a) Business registration

Every person carrying on business in URT is required to apply for business registration within before commencing business. This requirement applies to other types of entities, including sole proprietorships, partnerships and unincorporated bodies of persons, foreign companies and branch businesses of legal persons and legal arrangements. Mostly sole proprietorships and partnerships, such as law and accounting firms operate with a business registration certificate without a certificate of incorporation which is only granted to companies.

A Business License is obtained from the Ministry of Trade and Industry and for the purpose of obtaining a Business License one must submit the application accompanied with a Certified copy of the Memorandum and

Articles of Association or entity's constitutive documents; certified copy of a Certificate of Incorporation or relevant licence from the sector regulator; Certified copy of a TIN certificate; Certified copy of the Tax Clearance obtained from the Tanzania Revenue Authority; Certified copy of the Lease Agreement (stamp duty and Withholding tax paid) for the office; and Directors/ Shareholders ID/Passport copies. The requirement to submit the identification information of directors/shareholders is a mitigation on ensuring that the business entity is not used by criminals for ML/TF/PF purposes.

(b) Legal Persons (Companies)

All companies created in URT are required to be registered under both the Companies Act (Cap. 212) and the Companies Act, 2013 of Zanzibar. In Tanzania Mainland, the Registrars is required to keep a Registers containing all information about the companies created and identified by a company registration number. At the time of creating the company a statement is required by the Registrar in a prescribed form providing the name and address of the director(s) and secretary(ies) of the company and the intended address of the company's registered office upon incorporation. The Registrar is required not to register a company if information is missing. The Registrar, upon registration of the Memorandum and Articles of Association, has to certify under his hand that the company is incorporated and whether it is a limited or a public company. Similar provisions exist under the Companies Act 2013 of Zanzibar except that Registrar in Zanzibar, upon registration of the company is required to only state the type and if it is a limited company. A company incorporated in Zanzibar is

required within fourteen (14) days from the date of incorporation to provide the Registrar with the address of the registered office of the company.

A certificate of incorporation issued by the Registrars in both Tanzania Mainland and Zanzibar is conclusive evidence of a company being registered. Under both laws, the documents kept by the Registrar are all publicly available for inspection and obtaining of certified copies upon payment of a prescribed fee for members of the public and for free for competent authorities.

Companies in both Tanzania Mainland and Zanzibar are required to maintain registers of directors, who should provide information on their name, surname, usual address, nationality, business occupation, and in the case of a corporate, its corporate name and registered principal office. In both laws, companies are required maintain a register of its members with information on their name and address of each member and if it's a company having a share capital, a statement on the shares held by each member distinguishing each share by its number and where possible by its class, and the amount paid on the shares or agreed to be considered as paid for the shares of each member; the date which each person was entered into the register as a member or ceased to be a member. The register is to be kept at the registered office of the company and where the register of members is kept elsewhere other than the registered office of the company, the company shall notify the Registrar of the place where it is kept and of any change in that place, thereafter.

In 2020, the Companies Act,(Cap. 212) was amended through the Finance Act No 8 of 2020, to specifically require companies to deliver upon registration, a statement in the prescribed form containing, accurate and up to date records of beneficial owners of such company including their full name, any former or other name; date and place of birth; telephone number; nationality, national identity number, passport number or other appropriate identification; residential, postal and email address, if any; place of work and position held; nature of the interest including the details of the legal, financial, security, debenture or informal arrangement giving rise to the beneficial ownership; and oath or affirmation as to whether the beneficial owner is a politically exposed person or not. Beneficial owner according to the Companies Act means "a natural person who directly or indirectly ultimately owns or exercises substantial control over an entity or an arrangement; who has a substantial economic interest in or receives substantial economic benefit from an entity or an arrangement directly or indirectly whether acting alone or together with other persons; on whose behalf an arrangement is conducted; or who exercises significant control or influence over a person or arrangement through a formal or informal agreement."

By virtue of the Amendment in 2020, the Registrar of Companies holding specific BO information is mandatory and where there are changes in the beneficial ownership of the company, notice has to be given to the Registrar within thirty days of such changes.

Companies in both Tanzania Mainland and Zanzibar are required to keep information accurate and to be updated on a timely basis and they are required to file annual returns in a prescribed form within 28 days of the date

of the company's anniversary, audited accounts (with supporting documents attached), and timely report changes of any information provided to any of the Registrars at the time of registering the company. In both Laws, the Registrar, when necessary, can call for any information from the company.

In both Mainland Tanzania and in Zanzibar reporting entities, which include both financial institutions, DNFBPs and regulators are required to obtain information relating to BO as part of carrying out their CDD requirements under the AMLA and AMLPOCA as amended in March, 2022 [Refer: AMLA S. 15A (2) (a) and AMLPOCA 10B(a)].

The AMLA and AMLPOCA designate all regulators including registrars of companies as reporting persons. In that regard, the registrars of companies are required to identify the licensees at the time of licensing and obtain BO information. This requirement is a mitigation to the vulnerability and risk posed by other legal persons which may not be using financial institutions taking into account that both Mainland Tanzania and Zanzibar are largely cash economies.

In order to ensure companies have updated information Sections 128 and 129 which are basically requirements for furnishing returns requires companies to deliver to the Registrar, successive annual returns each of which must be made up to a date not later than the anniversary of the company's incorporation, or a different date if the company's last return delivered on another date than its anniversary. The return must be in a prescribed form and must be signed by a director or the Secretary of the company. If a company fails to deliver an annual return in accordance

with within twenty-eight days of the return date, the company and every officer of the company who is in default is liable to a fine and, in the case of a continued failure to deliver an annual return, to a default fine.

By virtue of section 129, every annual return shall state the date to which it is made up and shall contain, among others, information detailed company' information together with information about the beneficial owners not kept at the company's registered office, the address of the place where it is kept.

In both Mainland Tanzania Zanzibar, share warrants are allowed. As mitigation to ensure that share warrants are not misused for money laundering or terrorism financing purposes due to the fact that they have the effect of allowing bearer shares and mere share warrants and may be easily converted into registered shares or share warrants, the 2020 [4] amendments to the Companies Act of Mainland imposed a mandatory approval of the Registrar for their issuance and transfer. The provisions on mandatory registration are intended to ensure that the bearer shares and share warrants are immobilising and are held with a regulated institution.

In Zanzibar the Companies Act is in the process of being renewed to, among others, comply with international standards. Incidences of misuse of company for criminal intent are many and takes various forms.

Example: Mis-use of Companies/Legal arrangement

In 2018 Golden Globe International Services Limited owned by a prominent businessman, Yusuf Manji lost 34,479 shares in Mic Tanzania Limited, trading

[4] Finance Act No: 8 of 2020

as Tigo, purchased at TZS 13bn/. The Court of Appeal of Tanzania nullified the sale deal of the shares, made in 2014, in the execution of a court's decree in favor of a British national, James Alan Russell Bell, who was claiming to have been an employee of the mobile phone service provider. The Court of Appeal ruled in favor of Millicom (Tanzania) NV after holding that the execution process was flawed with material irregularities, which rendered the purported sale of the shares a nullity. The Court of Appeal set aside the purported sale and ordered the purchaser to be refunded the purchased price by whoever was holding the money," as the money was not in Court's record. The source of the dispute was in 2002, when a Briton, Mr. James Bell, filed a civil case against MIC UFA Ltd, Millicom International Cellular SA, and MIC Tanzania Limited. In the case, Millicom Tanzania NV was not a party. Mr. Bell, the Plaintiff in such proceedings, managed to get a default judgment against MIC UFA Limited and Millicom International Cellular SA in March 2005. The Plaintiff attempted to execute the judgment against shares in Tigo, but could not because High Court on November 7, 2009, ruled that such shares were not owned by Millicom International Cellular SA, but rather Millicom NV, a wholly separate legal entity. However, on February 18, 2014, the Plaintiff moved another action by filing an application for execution against the same shares, which he claimed were owned by Millicom International Cellular in Tigo. On June 17, 2014, a District Registrar appointed a court broker as auctioneer and issued a prohibitory order attaching shares of Millicom International Cellular owned in Tigo. The said attached shares were sold by way of an auction on November 5, 2014, to an offshore company, Golden Globe International Services limited, allegedly controlled and beneficially owned by Mr. Yusuf Manji. On November 10, 2014, the District Registrar issued a certificate of sale. It

appears that the buyer after realizing to have purchased shares that do not exist, moved the District Registrar to issue another certificate of sale, where the name of Millicom NV was inserted. The circumstances surrounding this 'editing' of the order strongly imply forgery or fabrication and serious misconducts. In essence, Millicom NV was 'added' to court proceedings by the stroke of a pen, without ever being a party to the case, without having heard, without being summoned to the court and in highly suspicious circumstances.

In view of the above, there is an inherent ML/TF/PF vulnerability to legal persons. However, there does not seem to be any visible impact affecting the overall risk in URT so far and therefore, the risk of legal persons is assessed as medium.

(c) Legal Arrangements

The law of trusts in URT is based on and derived from the English law of trusts. The common law concept of trust is in use in Tanzania subject to the mandatory registration requirements with the RITA of the Trusts. A trust may be defined as "the relationship which arises whenever a person (called the trustee) is compelled in equity to hold property, whether real or personal, and whether by legal or equitable title for the benefit of some persons (of whom he may be one and who are termed beneficiaries) or for some object permitted by law, in such a way that the real benefit of the property accrues, not to the trustees, but to the beneficiaries or other objects of the trust. The common law rule is that a trustee must execute the trust with reasonable diligence, and conduct its affairs in the same manner as an ordinary prudent man of business would conduct his own affairs. A higher

standard of care applies to a trust or similar body which carries on a specialized business of trust management.

In Mainland Tanzania trustees are regulated by the Trustees' Incorporation Act (Cap.318) and its rules. The office of Registration Insolvency Trustees Agency (RITA) is the regulator of the trusts. To incorporate a trust in Mainland Tanzania an application is submitted to the Administrator-General for incorporation accompanied with the constitution and rules trustees' particulars i.e., the CVs and passport size and IDs for each trustee; recommendations from the Ward Executive Officer, District Commissioner and Minutes of the meeting that passed the constitution and appointment of the trustees. The administrator-general may require the applicant to furnish an oath or otherwise or other evidence in verification of the statements and particulars in the application and any other evidence as the administrator-general may think fit and payment of relevant fees. Upon satisfaction, the administrator-general will register the trust and the trustee and issue a certificate of registration. After successful registration, the trust is transferred with the trust property to the trustee and then the trustee will start to manage the trust fund. Annual return must be filled by the trustee.

To mitigate the risks of trusts being used by criminals, the AMLA and AMLPOCA designated regulators in general as reporting person. In this regard, the registrars of trusts are reporting persons who are required to conduct CDD measures when they licence trusts. CDD in the laws of URT includes establishing the identity of the customer, beneficial owner or a person purporting to act on behalf of a customer. Beneficial owner in terms of trusts according to the Anti Money laundering laws in URT is the settlor, trustee or protector, the beneficiaries, or where the natural person

benefiting from the trust has yet to be determined, the class of natural persons in whose main interest the trust is set up or operates; or any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means. The trustee must exercise the care and skill that is reasonable in the circumstances, having regard to any special knowledge or experience that the trustee has or holds out as having and if the trustee is acting in that capacity in the course of a business or profession, any special knowledge or experience that is reasonably expected of a person acting in the course of that kind of business or profession. The duty of care imposed on trustees under the general law continues to govern the administration of trusts where the statutory duty of care does not apply.

Trusts can be used for both private (e.g. personal inheritance) and commercial purposes (e.g. fund management as is the case of Unit Trust of Tanzania). Any company incorporated in URT (which is not a private company) may apply to the Registrar of Companies to be registered as a trust company subject to certain requirements (including restriction of the company's objects to trust businesses. Registration by a trust company is voluntary. Express trusts are subject to registration requirements under the Trustee' Incorporation Act, (Cap.318) which is an exception to the common law principle which only requires trustees of any express trust to discharge a number of duties in the administration of the trust. Such duties include acquaintance with the terms of the trust and its affairs, conforming to and carrying out the terms of the trust, taking possession and preserving trust property, keeping an accurate account of the trust property and rendering the account when required.

There is little in the way of typology studies or data to suggest domestic trusts are being abused for ML/TF/PF purposes in URT. The NAMDC, taking into consideration the typology studies under taken by FATF and FSRBs takes note of the risks posed by foreign trusts particularly those forming part of complex multi-jurisdictional structures with links to or through URT. NAMDC places particular attention and apprise AML/CFT/CPF stakeholders in URT that complex corporate and trust-related structures are frequently used to evade tax, and can also be used to launder illicit funds. Such foreign trust structures thus pose medium to medium-high ML risks to the financial sector and DNFBPs in URT.

When misused, trust and asset management accounts can conceal the sources and uses of funds, as well as the identity of beneficial owners. Factors that can serve as indicia of a higher risk that the trust is being used for inappropriate purposes include unusual account relationships and circumstances, questionable assets and sources of assets, and other potential areas of risk, such as offshore accounts, private investment companies, and transfers of funds to or from offshore accounts.

To date, the available evidence does not indicate that trusts established within the URT are frequently used for money laundering purposes. Practice in other jurisdiction indicate that they are used for tax avoidance purposes by both citizens and foreign persons. While that is distinct from money laundering, it still is of interest to the NAMDC given that tax evasion is a predicate offence in URT. Where trusts have been identified as being used to launder money, they relied on the defense of being trustees willing to act illegally to provide a clean name for the trust documents. The NAMDC is

seeking to expand its understanding of whether and how trusts in URT are misused for illicit purposes.

The exact number of trustees in the URT is unknown as most trusteed legal arrangements are not registered and generally any natural person may serve as a trustee. The risk of trusts being misused for TF purposes is assessed as low given the mitigation through the registration requirements and CDD measures including identification and verification of BO.

3.2.1 Status of Beneficial Ownership Requirements

As defined by the FATF, the global AML/CFT standard-setting body, a beneficial owner is the "natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted." FATF also considers as beneficial owners "those persons who exercise ultimate effective control over a legal person or arrangement."

In the united Republic it is believed due to absence of research/investigation, that, criminals have historically been able to take advantage of the lack of uniform laws and regulations pertaining to the disclosure of information detailing an entity's beneficial owners, or beneficial ownership. This has stemmed mainly from the different levels of information and the transparency required at the time of a legal person or legal arrangement is licensed or registered by relevant registry.

Until recently, the URT has had major gaps in its legal and regulatory framework for the collection of beneficial ownership information, both by reporting persons, regulators and registries, leading the ESAAMLG to give the URT the lowest possible ratings in its MER 2021/22 for its lack of

transparency of beneficial ownership information, and failing to prevent legal persons and arrangements from being used for criminal purposes.

The URT has made significant progress in addressing the beneficial ownership information. The Amendments to both the AMLA and AMLPOCA requiring reporting persons to obtain BO information when establishing business relationships with legal persons and legal arrangements came into operation in March, 2022. This requirement helps mitigate the legal persons and legal arrangements vulnerability to ML/TF/PF.

The new requirements for the disclosure of beneficial ownership information once fully implemented, are expected to help facilitate law enforcement investigations and make it more difficult for criminals to hide behind corporate vehicles in the URT or those foreign entities registered to do business in the URT. The NAMDC take cognizance of the fact that criminal may still continue to take advantage of foreign legal structures lacking beneficial ownership disclosure requirements to obscure their illicit activity including those linked to foreign corrupt PEPs. These can continue to rely on the anonymity granted to beneficial owners of shell companies and other corporate vehicles that are not registered in the URT and that are within "black box" jurisdictions abroad that have strong corporate secrecy laws and legal frameworks that do not facilitate international cooperation.

3.2.3 Shell and Shelf Companies

Criminals have consistently used specific legal persons and legal arrangements to disguise criminal proceeds, and law enforcement agencies in URT have had no consistent way to obtain information about the beneficial owners of these entities. The ease with which companies can

be incorporated and the absence of BO information generally or the entities activities lead to limited transparency. Criminals take advantage of these lax requirements.

3.3 VIRTUAL ASSETS

Digital assets are a broad term that is used for virtual assets. Virtual assets include the so-called digital currencies, stable coins, or cryptocurrencies. Digital assets can be securities, commodities, derivatives, or other financial instruments. To align with the terminology defined by the FATF, the terms Virtual Asset and Virtual Assets Service Providers (VASP) are used herein.

In this report, virtual assets, include non-sovereign-administered digital assets such as convertible virtual currencies (CVCs), like bitcoin and stable coins but do not cover central bank-issued digital currencies CBDCs, which are representations of fiat currency. As in most jurisdictions, there is no specific regulation over Virtual Currencies (VCs) which are regarded as virtual commodities but not as a legal tender in URT. Transactions with VCs are in essence bilateral contractual arrangements between service vendors and users for bartering specific goods or services. Some VCs are highly speculative and prices may fluctuate widely due to speculation. They may not be backed by any physical item, issuers or the real economy and investors or consumers may suffer significant monetary losses as a result of the volatile prices.

Under the AMLA, a reporting person is required to conduct money laundering, terrorist financing and proliferation financing risk assessment associated with the use of new or developing technologies for both new and pre-existing products. New technology include any transfers within

decentralized convertible virtual currencies or assets networks, person-to-person transfers involving hosted wallet providers, large value virtual currency payments or assets transfer, mobile payments and internet-based payments services. When conducting risk assessment with respect of virtual currencies or virtual assets, reporting persons are required to pay particular attention to the risks posed by the nodes or points of intersection that are used to move value into and out of fiat currencies and shall focus the efforts on identifying higher risks convertible virtual currencies or assets.

All in all, URT is still a growing economy with adequate foreign currency exchange market and capital controls. VCs are not as attractive as in economies where people may try to circumvent currency controls or seek refuge from a high inflation rate. In addition, VCs are not legal tenders and are not accepted for payment in URT. The exchange of Bitcoin in person is not popular.

The NAMDC note that the market for VCs, in particular for Bitcoin, has undergone notable fluctuations triggered by speculation, as well as the introduction of regulatory framework over Bitcoin in other jurisdictions. Domestically, the use of Bitcoin remains at a negligible level and monitoring of financial flows no apparent sign of organized crime or ML/TF concerning trading of VCs. In this regard, the threat level is low.

The NAMDC also note that the anonymous and decentralized nature of some VCs poses potential ML/TF risks. There are some banks that are alleged to exchange Bitcoin to fiat currency and some online exchange platforms allegedly based in other jurisdiction. They are not openly used by people in URT and therefore monitoring them for AML/CFT/CPF purposes is

difficult. The NAMCD also take note of the growing trend in criminals' use of anonymity-enhancement technologies, such as enhanced cryptography or operation on an opaque blockchain, in the virtual asset sector. These are assets or services, such as mixers or tumblers, that help criminals hide the movement or origin of funds, creating additional obstacles for investigators. Anonymity-enhancement technologies create challenges for investigators attempting to trace illicit proceeds. Illicit actors have shown an interest in the use of virtual assets and services specifically designed to obscure transactional activity and limit transparency. For example, Monero as a form of cryptocurrency is said to obfuscate transaction information using cryptographic technologies, such as ring signatures, which are used to hide the identity of the transaction originator; or ring confidential transactions, which obfuscate the amount of the transaction; and stealth addresses, which hide the identity of the beneficiary. These transactions are not broadcast publicly on the Monero blockchain. Instead, they use one-time generated addresses to conceal both the sender and beneficiary to external entities. With every new transaction, ring signatures obfuscate the origin of the funds by mixing values with a minimum number of other transactors, creating challenges for investigators tracing illicit funds such as ransomware proceeds.

To raise public awareness of the inherent risk of VCs, the NAMDC Government and the regulators will continue to issued warnings on ML/TF/PF and cybercrime risks associated with VCs.

The current legal and regulatory provisions relating to ML, TF, PF, fraud and other crimes are wide enough to catch offences involving the use of any general property, including VCs. As regards prevention of ML/TF/PF, all

natural and legal persons have statutory obligations to file STRs in relation to any property.

In view of the above, although there is inherent ML/TF/PF vulnerability related to VCs, there does not seem to be any visible impact affecting the overall risk in URT so far. The risk of VCs is assessed as medium-low.

The NAMCD take note of the growing trend in criminals' use of anonymity-enhancement technologies, such as enhanced cryptography or operation on an opaque blockchain, in the virtual asset sector. These are assets or services, such as mixers or tumblers, that help criminals hide the movement or origin of funds, creating additional obstacles for investigators. Anonymity-enhancement technologies create challenges for investigators attempting to trace illicit proceeds. Illicit actors have shown an interest in the use of virtual assets and services specifically designed to obscure transactional activity and limit transparency. For example, Monero as a form of cryptocurrency is said to obfuscate transaction information using cryptographic technologies, such as ring signatures, which are used to hide the identity of the transaction originator; or ring confidential transactions, which obfuscate the amount of the transaction; and stealth addresses, which hide the identity of the beneficiary. These transactions are not broadcast publicly on the Monero blockchain. Instead, they use one-time generated addresses to conceal both the sender and beneficiary to external entities. With every new transaction, ring signatures obfuscate the origin of the funds by mixing values with a minimum number of other transactors, creating challenges for investigators tracing illicit funds such as ransomware proceeds.

The NAMDC will continue to review the ML/TF/PF risk of VC and VASPs and their risk assessment will be reviewed in the light of regulatory experience and operational data for the sector as it becomes available. The NAMDC and the regulators will monitor further developments, including the use of VCs in URT, the evolving international regulatory consensus, and regulatory and enforcement actions in comparable jurisdictions. A landscaping exercise will be conducted to assess ML/TF/PF risk and recommend action if necessary to ensure public protection and prevention of crime.

3.4 COMPLICIT DNFBPs

Criminals seek out complicit professionals and financial services employees to help effectuate their money laundering schemes. This occurs when professionals abuse their professional position to aid criminals through facilitating Trade Based Money Laundering (TBML). The professionals include attorneys, real estate agents, and financial services employees, among others.

3.4.1 Lawyers (Advocates)

Lawyers are normally engaged in activities identified by the FATF to be at risk for ML/TF/PF, providing a range of services covered by the FATF Recommendations including conveyancing (real estate transactions), trustee services, services relating to the formation and administration of companies and entities, and the buying and selling of businesses.

Practicing advocates are not prohibited to accept any instructions to receive, disburse or otherwise handle clients' money, securities or other

assets on payment of fees and are hence involved in activities covered by the FATF Recommendations.

Advocates are licensed by High Court of Tanzania and in Mainland are registered as members of the Tanganyika Law Society. In Zanzibar, the Zanzibar Law Society is the regulator of all lawyers. Advocates are bound by professional codes of ethics. Some maintain bank accounts in their own name for client use (mostly trust/escrow accounts in which clients' funds are held for future transactions. Others act in an advisory capacity and may handle funds associated with settlement checks or trusts that they administer on behalf of their clients, while others may work on behalf of large corporations.

Advocates in URT are subject to AML/CFT measures as reporting persons by virtue of the Anti-Money laundering laws. However, they are not obliged to any cash transactions reporting. In this regard, they may not adequately address ML/TF/PF vulnerabilities and do not reporting of suspicious activity to FIU despite the provisions of the law. In addition, there is no enforceable mechanism to compel them to follow voluntary best practices guidelines nor mechanisms which would result in the issuance of civil or criminal penalties for failing to comply with these practices.

Although there not many reported cases on how complicit lawyers have been used for ML/TF purposes.

Example:

The celebrated case of the Arusha based advocate is one example. In the said case, in December, 2018, the court fined a popular Arusha lawyer

Median Mwale TZS 200 million or serve five years in jail for money laundering charges for the charge of laundering USD 5,296,327,25 (TZS 15 billion) forged US Treasury cheques. He was charged alongside Kenyan politician Don Bosco Gichana and CRDB Bank managers Boniface Mwimba and Elias Ndejembi who facilitated the laundering processes. Mr Gichana was set free after paying Sh300 million in fine after pleading guilty to the offence. Both Mwale and Gichana changed their plea, with the mwale pleading guilty on November 28, 2018. The CRDB Bank employees maintained they were not guilty charge. Mr Mwale a popular figure in Arusha and the bank officials were arrested and arraigned over 42 charges of money laundering, conspiracy, forgery and possessing property obtained through illicit means.

The TLS and the ZLS are designated as the regulatory bodies for monitoring and supervising the compliance of legal professionals with the AML/CFT/CPF requirements.

Based on the assessment in the previous NRA, the level of ML/TF/PF risk for lawyers is assessed to be medium, comprising a medium-low level of ML threat and a medium level of ML vulnerability.

3.4.2 Accountants

The National Board of Accountants and Auditors NBAA is authorized by the National Board of Accountants and Auditors Act to issue practicing certificates to certified public accountants ("CPAs"), which enable them to perform auditing work for companies. The NBAA is also responsible for regulating the professional conduct and standards of its members (including conducting practice reviews, taking disciplinary actions and imposing sanctions), setting codes of ethics and standards of accounting

and auditing, regulating entry to the profession through its qualification programme, providing continuing education and other services to members, and promoting the accountancy profession in URT and overseas.

CPAs commonly provide trust or company services, although predominantly through separate legal entities because of the need to maintain independence from their statutory auditing duties. They are thus also subject to the ML threat associated with TCSPs. Typologies however do not suggest any noticeable threat to such "traditional" activities as auditing or tax advisory services.

CPAs are members of a profession generally known to place considerable emphasis on ethics, integrity and a culture of compliance and NBAA also makes continuous and consistent efforts to oversee the professional conduct of its members and their compliance with its rules and regulations, and promote good practices.

Most of the large Accounting and Auditing firms have already established stringent and comprehensive AML/CFT measures, particularly on the acceptance of clients. Practices which are part of international networks of firms commonly embrace AML/CFT policies and controls designed to meet the FATF's requirements. On the other hand, the level of AML/CFT controls among smaller firms, including sole proprietorships, varies.

Pursuant to AMLA and AMLPOCA Accountants are subject to statutory requirements to file STRs.

Professionals in the sector generally believe that the low STR numbers are a positive outcome of the stringent screening process of onboarding.

Dubious clients would have already been screened out before establishing a business relationship, thus substantially reducing the likelihood of suspicious transactions.

Meanwhile, as accounting professionals engage in the riskier TCSPs business usually operate in separate entities, the STR numbers might have been counted under the TCSP category.

Given the available mitigating preventive measures including the CDD requirements that apply to the accountants, the level of ML risk for accountants is assessed to be medium, comprising a medium-low level of ML threat and a medium level of ML vulnerability.

3.4.3 Real Estate Agents

For a long time, real estate agents in URT are not regulated in terms of there being a legislation or having a regulator to regulate and supervise the practices of the real estate agency trade or to promote the integrity and competence of estate agents, and enhance the status of the trade. An individual or company carrying on estate agency work normally operate on the basis of a business license. The main role of estate agents in real estate property transactions is to act as middlemen between potential seller and buyer, arranging property viewings and witnessing the signing of agreements for rent/lease, sale and purchase of real estate.

Real estate agents commonly have face-to-face contact with purchasers and sellers, allowing them to acquire knowledge of the background of their clients. In most, if not all cases, the estate agents' role in handling clients' money is very limited to (in very rare cases) to passing the purchaser's initial

deposit to the seller or the seller's solicitors upon signing of the provisional agreement for sale and purchase. A common practice in URT is for the purchaser to effect payment directly to the seller on cash or through the seller's account. Payment of the initial deposit in cash is rare in URT. After agreeing to the sale and purchase, an agreement will be signed and payment will accordingly be made depending on the agreement. The purchase price invariably involves conveyancing lawyers and banks.

High-risk real estate transactions include those involving the purchase of high-value property, the use of legal entities to conceal the ultimate owner, all-cash purchases, and the use of intermediaries who are not covered by AML obligations.

Given the relative stability of the real estate sector as a store of value, the depth of the real estate market, and gaps in industry regulation, the URT real estate market continues to be used as a vehicle for money laundering and can involve businesses and professions that facilitate (even if unintentionally) acquisitions of real estate in the money laundering process. The real estate sector therefore represents a significant vulnerability that can facilitate money laundering schemes related to a wide range of crimes and evasion of penalties. The use of real estate in money laundering is believed to affect prices in certain real estate markets; when bad actors deliberately overpay for property, prices can rise, putting legitimate buyers and sellers at an economic disadvantage.

The purchase of real estate may also provide a reliable way for criminals to store or conceal illicit proceeds in an appreciating asset while also benefiting from greater opportunities for anonymity compared with other

financial assets. This anonymity is particularly easy to achieve if buyers do not need a mortgage loan and purchase the property in the name of a legal entity, as there is no collection of information on the true buyer and limited or no AML/CFT/CPF safeguards.

In most of the cases in URT, the real estate transactions are cash transaction where buyers make purchases without a real estate agent, insurance or financing through a financial institution or mortgage company, or an attorney to close the deal.

The risks in real estate sector are compounded in transactions involving commercial real estate, as there are additional types of purchasing options and financing arrangements available for parties seeking to build or acquire property worth hundreds of millions. Lawyers, accountants, and individuals in the private equity fields, typically facilitate commercial real estate transactions, often working at different stages of the deal and operating with different beneficial ownership and financial information related to buyers and sellers.

In commercial real estate, the use of purpose-built legal entities and indirect ownership chains is the norm as parties create tailored corporate entities to acquire or invest in a manner that limits their legal liability and financial exposure. The result is an obscured or concealed field of diverse foreign and domestic legal entities associated with transactions worth hundreds of millions of monies.

While there may be legitimate reasons for some buyers such as high-net-worth individuals to use a legal entity, intermediary, or other means to seek

privacy from the public in a real estate transaction, these vulnerabilities are extremely useful to criminals. At the same time, less sophisticated criminals seeking anonymity may also use less complicated nominees, such as a friend or relative, to own property on their behalf to conceal illicit proceeds.

NAMDC will continue to gather more information about money laundering risk in the real sector to ensure that specific guidelines are issued targeting certain geographic areas or high-risk locations that often see significant real estate money laundering activity requiring persons involved to identify the natural persons behind legal entities used in all-cash purchases of real estate. The purchase amount threshold should also be legislated to ensure consistency on prices of real estates.

The sector is rated with High vulnerability given its reliability as the sort of value, and appreciating price nature.

3.4.4 Dealers in Precious Metals and Stones

Mining is a leading industrial sector in Tanzania with the value of mineral exports constantly increasing for the past several years. The sector is comprised of both small- and large-scale operations. Mining in Tanzania includes metals (gold, iron ore, nickel, copper, cobalt, silver), industrial minerals (diamonds, tanzanite, ruby, garnet, limestone, soda ash, gypsum, salt, phosphate, gravel, sand, dimension stones and graphite), and fuel minerals (coal, uranium). Tanzania is also home to many rare earth and critical minerals that are currently in the exploration stage. Gold is the one of the most mined minerals commodities that highly contribute to the government revenues. Gold exploitation is done by both large and medium scale minors as well as smaller miners thought the country

Tanzania earned around 2.3 billion U.S. dollars with minerals exports in 2019, a significant increase over 2018 level of 1.6 billion U.S. dollars. Gold had the highest contribution to the value of mineral exports. Tanzania is the 4th largest gold producer in Africa after South Africa, Ghana and Mali and is the world's sole producer of the precious stone Tanzanite. Gold production currently stands at roughly 40 tons a year, copper at 2980 tons, silver at 10 tons and diamond at 112,670 carats. In 2019/2020 a total of 53.53 tons of gold valued at TZS 5,864.05 billion were produced and sold of which 38.20 tones (TZS 4,350.20 billion) were from large mining and quarrying activities had a very large contribution to Tanzania's Gross Domestic Product (GDP) growth in the first quarter of 2021. The sector recorded 10.2 percent of the GDP equivalent to 1,473,804 million TZS.

Dealers in precious metals and stones ("DPMS") in URT can be roughly divided into three categories: retail, wholesale and metal exchange. According to 2019-2022 Commission report TZS 528.36 billion revenues was collected from the mineral sector which was an increase of 52.6% from the previous year. Mineral licenses granted were 7,214 and TZS 104.63 billion were revenue collected from mineral government houses (mineral markets).

Mineral license (Dealing) gives the holder the right and authority to engage in a business of minerals and trade as a broker or a dealer after having met the legal requirements prescribed by the law. Type of Mineral licenses issued in Tanzania are Broker Mineral license (a holder is authorized to buy or acquire gold or, as the license may specify gemstones from an authorized miner and sell or dispose of mineral or minerals so acquired to a

licensed Mineral dealer. A broker license restricts the holder to export any mineral or minerals outside the country. He is only authorized to buy minerals from small miners and sell them to the licensed mineral dealers, the reason being to facilitate the transaction and collection of minerals from small miners to large scale sellers and exporters i.e. minerals dealers); Dealer Mineral license (a holder has the right to acquire or buy minerals from Licensed miner or licensed Broker, also, sell, dispose or Export Mineral or Mineral Products, outside the country. Upon application and meeting the legal requirement can be granted the export permit to export the mineral or mineral products outside Tanzania.)

Eligibility criteria is to be a body corporate incorporated under the Companies Act having the objectives of conducting mineral business and having at least 25% of share owned by Tanzanians; one director be Tanzanian; control of company, both direct and indirect should be exercised from Tanzania by Tanzanians and the company should not be in a liquidation or in a winding/dissolution process.

The Mining Commission is responsible for issuing licenses for mining and minerals dealings. An application for a dealer and broker license is addressed to the Commissioner of Mineral in the prescribed form accompanied by a commitment statement indicating the capacity to undertake the business. Business license is also mandatory and as indicated in part on legal persons that the requirement for grant of business license contain some aspects of CDD including proof of Tanzanian Citizenship for members and directors of the company and proof of suitable company premises i.e. the place of business of the company must be in Tanzania and

Registration of social security numbers from all mandatory social security schemes.

URT operates a precious metal exchange market, with availability of physical precious metals. The import and export of gold, precious metals and stones are governed by the Mining Commission and associated regulations. Controls are in place with respect to declaration and manifestation for imports and exports; registration and certification of the traders; regulation of the standard of fineness of precious metals (i.e. gold, gold alloy, and platinum); and protection of intellectual property rights.

The regulatory regime helps reduce the risk of misuse of the sector for ML/TF/PF purposes as, for instance, an audit trail of the precious metals and stones can be established as and when necessary.
The threat in this is that crime proceeds can be converted into precious metals and stones. Further conversion of crime proceeds from precious metals and stones to other forms is also a possibility as crime proceeds may be embedded in precious metals and stones and no dealer can be linked to it.

The vulnerabilities in this sector are large cash transactions that are a key facet of the risk for DPMS. In the retail sector, cash transactions are still found and they are increasingly being substituted by deposits in bank accounts as seen in STRs received from banks. Lower-value precious stones are found to dominate the retail market.

All in all, this sector's reporting persons have not started applying AML/CFT/CPF preventive measures such as identifying risky transactions

and verifying customers' identity, especially for transactions that involve large amounts of cash.

On the wholesale side, dealers tend to trade with reputable and reliable business partners with whom they have established long-term relationships. On the precious metal exchange, settlements are generally cash-based.

Dealers in precious stones and metals are designated as reporting person under the AMLA and AMLPOCA to carry out CDD, have internal procedures for on boarding customers, record-keeping, submission of STR/SAR and undertake continued professional development programs/training.

The NAMDC will continue to support all initiatives to ensure outreach and other capacity building of DPMS is carried.

In view of the highlight of the threat and vulnerability of this sector discussed above, the level of ML/TF risk for DPMS is assessed to be medium-low to medium, comprising a medium-low level of ML threat and a medium-low to medium level of ML vulnerability.

Although the ML risk of the DPMS sector is assessed as relatively low among the DNFBPs, it needs to be continuously monitored because of suspicious cases of smuggling of precious metals, mainly gold and silver to destinations such as Dubai. Also, because of rampant cash usage and potentiality of artisan miners operating illegally the vulnerability is rated Medium High. Smuggling is a predicate offence and laundering of crime proceeds

remain to be further investigated and studied. The LEAs should keep a close watch on the situation.

In conclusion of this part, an enhanced AML/CFT awareness of the DNFBP sectors is evident very low and no STR are received from this sector. To enhance AML/CFT regulation of DNFBPs, the National Strategic Plan has included a number of outreach and awareness programs for DNFBPs.

3.5 COMPLIANCE DEFICIENCIES

While many regulated financial institutions in URT have adequate AML/CFT programs, compliance deficiencies at these institutions continue to be a money laundering vulnerability.

3.5.1 Regulators

Despite noncompliance with AML/CFT/CPF measures, no enforcement actions have been taken by regulators such as cease-and-desist orders, warnings or remedial action plans. The AMLA and AMLPOCA have express provisions empowering regulators to variety of administrative sanctions.
This supervisory approach such as joint statement on the enforcement or joint on-site inspections are not common and regulators should start using these tools to ensure implementation of an effective AML/CFT/CPF regime.

3.5.2 Banks

AML-related deficiencies issues that have been identified stem from: inadequate CDD and enhanced due diligence (EDD), insufficient customer risk identification, and ineffective processes related to suspicious activity monitoring and reporting, including the timeliness and accuracy of SAR filings. Talent acquisition and staff retention to manage AML/CFT/CPF

compliance programs and associated operations present ongoing challenges, particularly at smaller and community banks.

Due to the size of banks in the financial sectors and attractiveness to perpetrators to abuse the sector, the vulnerability is rated Medium High.

3.5.3 Money Services Businesses

MSBs are frequently used by customers who would otherwise have difficulty in obtaining financial services, including many who are sending critically needed remittance payments. NAMDC remains concerned about the risk that many MSBs, including VASPs, may not be compliant with one or more of their AML/CFT/CPF obligations including those which are operating without required proper licenses or registration. Due to its mobility, ease of transacting and use of modern and technology the vulnerability is Medium High.

An examination needs to be conducted and proposal need to be made on AML supervision mechanisms for MSB for Small Business/Self-Employed. URT continues to see cases of MSBs which operate without required registration or licensing and therefore fall outside AML/CFT regulation and supervision. In addition, there is a need to address the whole question of VASPs.

3.5.4 Securities Market intermediaries

All securities market intermediaries are subject to AML/CFT/CPF requirements including having an AML program, a customer identification program, CDD, Cash Transaction Report, and Suspicious Activity/Transaction Reporting rules, as well as record keeping

requirements. The major deficiency in the securities market intermediaries sector include suspicious activity detection and reporting, customer identification programs, as well as AML program failures, including independent testing and ongoing training. The regulator has also not taken any enforcement actions related to deficiencies in the detection and reporting of suspicious activity. The regulator has not issued any AML/CFT/CPF regulations or guidelines on the various risks arising from dealing in securities. The sector is rated Medium Low

3.5.5 Casinos

A casino is an entertainment venue that offers its patrons gaming activities and some financial services to their customers. Gaming operators are subject to comprehensive AML requirements pursuant to the AMLA and AMLPOCA. The gaming environment is complex for AML compliance with sports betting and online gaming ever increasing. However, the AMLA and AMLPOCA have designated gaming operators as reporting persons for purpose of conducting CDD on them even in the context of online gaming.

Study conducted by FATF and FSRBs show that illicit proceeds earned from drug trafficking, illegal gambling, and fraud are placed in casinos directly as cash and casinos remain a popular way for launderers to hide their drug proceeds because of their high volume of currency transactions. A trend that has been observed is what is known as "chip walking." For example, in multiple jurisdictions, one target frequently gambled at a casino with cash from sex trafficking. The target took large sums of casino chips and left the casino in one city and drove to a casino in another city to play with those chips. The target did not cash out but left the casino again with large sums of chips he handed off to a second target at the casino. The other

frequently cited suspicious activities include transaction(s) below CTR threshold is unknown source of chips where two or more individuals working together, alter or cancel transaction to avoid CTR requirements and suspicion concerns source of funds.

Additional analysis of trends of suspicious activity involves gambling in huge sums of cash, sports betting, abandoned jackpot, and bill stuffing. The sector is rated Medium Low

3.5.6 Luxury and High-Value Goods

(a) Real Estate

It is not certain that most purchases of real estate in the URT involve funds derived from legal means, and most purchases serve a legitimate purpose and therefore, it is believed that real estate transactions are vulnerable to abuse by illicit actors seeking to launder criminal proceeds, including the proceeds of foreign corruption. The sector is rated Highly vulnerable

(b) Precious Metals, Stones, and Jewels

Persons involved in the trade in precious metals, stones, and jewels (PMSJs) are a diverse group, consisting of large-scale mining interests, artisanal and small-scale mining, traders, refiners, manufacturers, designers, retailers, and secondary markets such as pawnshops and auction houses. In URT, PMSJs engaged in the purchase and sale of jewels, precious metals, or precious stones are generally required to comply with AML reporting obligations. While these reporting obligations are significant, the current framework for precious gems dealers still presents a vulnerability for bad actors seeking to launder their illicit proceeds. Like other high-value assets, PMSJs may provide money launderers the opportunity to transfer the value of their illicit

proceeds into an easily transportable and concealable asset. Additionally, criminals may view PMSJs as an attractive laundering tool allowing them to conceal illicit wealth without increased scrutiny, because the underlying commodity is legal.

From a smuggling perspective, PMSJs can be transported across international borders by couriers on their person or hidden in other items, making it difficult for law enforcement and customs personnel to detect these items. Additionally, even upon detection of PMSJs, it is difficult for government officials to identify the origin of the PMSJ, impeding law enforcement investigations. This is particularly concerning when considering that some diamonds and other gems that can easily be purchased are valued over $100,000, which makes the concealment and smuggling of those purchased via illicit proceeds a money laundering vulnerability. The sector is rated High.

3.6 TERRORIST FINANCING

The assessment of terrorist financing vulnerability and risks has taken into account all relevant considerations, including the extent of terrorism threat in URT, the risk of the place being abused for TF activities, and the strength of CFT work in URT.

3.6.1 Terrorism Threat

Both Governments in URT are committed to combating terrorism and ensuring the country is a safe place for all. The two government adopt counter-terrorism policy that focuses on prevention and maintain comprehensive contingency plans for response to terrorist incidents.

Counter-terrorism is an operational priority of the Ministry of Home Affairs, with emphasis being placed on prevention, preparedness, response and recovery.

Tanzania faces terrorist threats on three of its borders with the Democratic Republic of the Congo, Kenya, and Mozambique. ISIS-Mozambique poses the greatest threat to Tanzania, having conducted at least two attacks inside Tanzania in 2020.

Examples:

Tanzania experienced two notable terrorist attacks in 2020 as follows:

- On October 14 an estimated 300 ISIS-Mozambique fighters attacked Kitaya village in Mtwara Region, which borders Mozambique. Attackers looted and burned houses, shops, vehicles, and an administrative office building. Attackers killed an estimated 20 people, including two security personnel. On October 15, for the first time, ISIS media claimed the attack inside Tanzania.

- On October 28, ISIS-Mozambique fighters attacked Michenjele village in Mtwara Region, 25 miles from Kitaya. Attackers looted and burned homes, shops, and infrastructure. Attackers killed five people and kidnapped an unknown number more. In an exaggerated claim, ISIS issued a statement on October 30 saying its fighters had attacked three villages in Mtwara near the "artificial border" with Mozambique.

In response to growing ISIS-Mozambique activity in early 2020, the Government of Tanzania sent additional security personnel to the border regions of Mtwara and Ruvuma, as well as to neighboring Lindi

Region. Following the October attacks in Mtwara, high level Tanzania's authorities signed an MOU that allowed extradition of terrorist suspects, greater information sharing, and joint operations against terrorism in northern Mozambique. As part of the MOU, Tanzania planned to extradite to Mozambique 516 persons detained in Tanzania for alleged cooperation or involvement in attacks in Mozambique's Cabo Delgado Province. In addition, Tanzania's announced that police had arrested an unspecified number of people from around Tanzania who were planning on travel to Mozambique to join the terrorists.

In 2020 the government of Tanzania continued with efforts to regulate the movement of foreign exchange which measures also make it easier to trace transactions, including those associated with money laundering and TF.

The situation in Cabo Delgado is one of complex social, economic, and ethno-religious dynamics. A deep feeling of social injustice and discrimination along religious and ethnic lines fueled the perception of the state's failure to deliver public goods. In fact, when the insurgency first started, the targets were government buildings and administrations. Attacks on churches came at later stages. The jihadists, affirming their willingness to impose Islamic rule in the region, find their support among unemployed and marginalized young people, who are easily radicalized.

The Macondé in Cabo Delgado have traditional links with Makondé in Tanzania. Mwani is a similar language to Swahili and Mwani speakers have traditional links to Zanzibar and coastal cities further north. The Makua and Yao are two large Bantu tribes of Southern Tanzania and northern

Mozambique. Tanzania's Mtwara Region and Cabo Delgado are inextricably linked through ties of family, language, faith, and economy. An effectively open border is straddled by families rooted on either side. A common language, Swahili, binds communities, while shared faith too ignores borders. Those elements made it easier for the insurgents on the Mozambican side to interact with their counterparts in Tanzania and vice versa, and to conduct small-scale attacks. It has also created an easy entrance for Tanzanians and other foreign fighters who take advantage of the lapse border security facilitated by a sense of brotherhood between the people of the two countries easily cross to Mozambique to join up insurrection in Cabo Delgado

The Recent emergence of terrorist perpetrating terrorist attacks in Tanzania borders through homegrown terrorists or foreign terrorist fighters operating alone or in small cells is seriously noted. All Tanzania neighboring countries may face terrorist threats from Al Shabab and other terrorist groups as is the case with Mozambique given the demographic, geographic and economic position of Tanzania. No one can guarantee that URT is immune from terrorist activities. However, there have been no terrorist attacks in URT in other neighboring countries or known activities of domestic or foreign-based terrorist groups. There has also been no specific intelligence or information to suggest that URT is likely to be a target of terrorist attacks. There is no intelligence indicating signs of self-radicalization. The Government assesses that the overall level of terrorism threat in URT is "moderate" meaning that there is a possibility of terrorist attack, but there is no intelligence suggesting that URT is likely to become a target.

3.6.2 TF Threat

The prevalence of terrorism worldwide has propelled the international community to make the fight against TF a priority. The FATF has identified that terrorist groups or organizations use funds for five broad purposes that are Operations; Propaganda and recruitment; Training; Salaries and member compensation; and social services. According to the FATF, traditional TF methods and techniques include abuse of donations and NPOs, funding from criminal or legitimate activities, physical transportation of cash and the use of bank accounts and MSOs are still prevalent. In addition, the financing of foreign terrorist fighters has become a prominent issue, and social media platforms and new payment products and services have been exploited for TF. A recent assessment on Australia, Indonesia, Malaysia, the Philippines, Singapore and Thailand found that terrorist funds in the region are more likely to be used for operational than organizational expenditure. Self-funding through legitimate sources for TF (particularly for foreign terrorist fighters travelling to or operating in conflict zones), raising funds through NPOs and cash smuggling to move funds are areas prone to high TF risks.

Although level of terrorism threat in URT is "moderate", the potential threat of financing domestic terrorism is medium. The threat of financing terrorism abroad (including for foreign terrorist fighters) may be greater, given URT open financial system, as well as the cultural and economic connectedness between certain segments of the community and regions affected by terrorism including Kenya and Somalia and security situations in DRC Congo.

TF-related STRs and investigations are mainly concerned with the use of bank accounts in suspicious movement of funds. STRs and investigations as well as TF-related MLA requests have not led to confirmation of any TF activity in URT, or discovery of high-risk patterns such as self-funding from legitimate sources, abuse of NPOs, or physical movement of cash across boundaries in URT. There have not been any cases that require the invoking of the freezing power or the TF offences provisions under the POTA. Nevertheless, as an all-reporting person in URT must guard against possible TF by persons locally or from abroad.

As regards the use of technology for TF purposes, available information does not indicate that social media platforms, VCs, online payment systems, prepaid cards, crowdfunding or other new payment methods have been exploited for TF purposes. However, as these platforms and products are evolving very fast, it is important to keep a close watch on their potential to be misused for TF.

TF-related STRs are filed to the FIU as a mandatory requirement under the AMLA, AMLPOCA and the POTA.

Between 2019 and 2021, there were two-related STRs. These mainly involved false-positive name or alias hits of known terrorists or terrorist associates, or financial transactions related to entities in high-risk jurisdictions. During the same period the FIU did not received intelligence from FIUs of other jurisdictions on fund transfers to URT by persons suspected to be linked to TF. There were no TF-related STRs and other information dissemination to the LEAS for immediate investigation as a matter of priority during that period.

The National AML/CFT/CPF Strategic PFIU's has identified manpower and capacity building to FIU and LEAS to further strengthen their ability to combat TF.

URT not received any MLA requests relating to TF between 2019 and 2021, and neither had URT assisted other jurisdictions request in conducting preliminary background enquiries, nor in finding actual TF taking place in URT.

The TF threat of URT is assessed as medium-low. There is no confirmed case of TF activity in URT. The nonexistence of MLA or other information requests supports this understanding. But in view of the moderate terrorism threat, the global and regional TF landscape, and the nature of URT geographical location neighboring terrorism troubled areas, the threat of TF taking place in or through URT cannot be completely ruled out and URT must continue to be vigilant and constantly monitor the TF trends.

TF Vulnerability in URT may stem from non-implementation of UNSC sanctions in URT. POTA and the regulations made under the POTA in 2022, implement counter-terrorism and sanction measures imposed by the UNSCR in particular the decision of the UNSCR 1373 requiring states to freeze the assets of terrorists and prohibit their nationals and persons within their jurisdiction from making funds, resources or financial services available to them. The regulations specifically implement targeted financial sanctions and other sanction measures against places designated by the UNSC, including Afghanistan, Iran and DPRK. The regulations also implement the FAT's Recommendation 6 that requires jurisdictions to freeze without delay

the funds or other assets of a person or entity designated as a terrorist or terrorist associate.

Further the 2022 POTA regulations implement the FATF Recommendation 5 that requires countries to mirror the UNSCR 2178, by criminalizing terrorist financing to include financing the travel of foreign terrorist fighters and the FATF's recommendation to enhance the freezing mechanism of terrorist property.

The vulnerability to international TF trends in URT stems from self-funding from legitimate sources for financing terrorist activities which is a growing issue for TF internationally. In URT, there could be concerns that financial institutions particularly banks and mobile phone are at risk, as people remit monies within and outside URT. The financial regulators continue to monitor compliance by banks and mobile phones with the AML/CFT obligations, and to promote awareness of TF among reporting persons, which already use multiple sources such as terrorist lists issued by the UN and other jurisdictions, specific AML/CFT databases, open sources and transaction monitoring to identify suspicious transactions.

The risks of NPOs being misused to move funds to terrorist organizations in other jurisdictions have been well recognized by the FATF. However, there has been no report of NPOs or charities in URT being misused for TF purposes, or found to sympathize with or condone terrorism, or linked to known or suspected terrorist groups. In addition, there is no intelligence or evidence from STRs, investigation or MLA requests suggesting that NPOs in URT are being exploited for raising or moving funds for TF. On this basis, there is no apparent TF threat identified for the NPO sector in URT.

In URT, NPOs may exist in various forms including societies registered under the Societies Act, companies, trusts, charitable bodies and other legal arrangements. NPOs are subject to the regulatory and governance requirements under various laws depending on their legal structure, their activities and funding sources. The regulatory regimes are not mutually exclusive. Where public funding is involved, there are stringent controls including submission of regular reports and audited statements by NPOs to regulators to ensure transparency and accountability.

In relation to those charities whose tax exemption status are recognized, the TRA conducts periodic reviews to ascertain whether they continue to be eligible for tax exemption status under the Income Tax Act.

The NPOs' attention has been drawn to the designated names of terrorists or terrorist associates and LEAs in URT have the powers to obtain information from Government departments concerned if necessary for counter-terrorism or CFT purposes. The inherent TF vulnerability of NPOs in URT is low, having regard to the current regulatory regimes and governance, the landscape of terrorism and TF threats as well as the focus of the majority of NPOs in URT.

With reference to international TF typologies and the local context, organizations operating and raising funds in URT for the purpose of supporting humanitarian services in conflict zones could be susceptible to TF risks. Nevertheless, these NPOs are commonly part of the international charities network to which the funds raised are disbursed, and have to a large extent put in place internal due diligence controls on their own.

Efforts will continue to be to ensure that Banks as well as all financial institutions are aware of the potential TF risks associated with the NPO sector in order for them to be able to monitor closely for funding or transactional patterns which may give rise to higher risks.

The overall with respect to TF vulnerability, URT has a sound legal and institutional framework to counter TF activities which is commensurate with the identified terrorism threat. The overall TF vulnerability is assessed as medium-low while URT has a medium-low TF risk with threat and vulnerability both rated as medium-low.

While URT faces a relatively low TF risk, the situation must be closely monitored, with current preventive measures kept under constant review. Policy makers, financial regulators, professional bodies and associations, the FIU and LEAs will continue to raise awareness of TF activities and emerging issues.

The legislative initiatives pursued by the Government recently will greatly strengthen the CFT framework and further alleviate the TF risk. The AMLA and AMLPOCA which extends statutory CDD and record-keeping requirements to legal professionals, accounting professionals, TCSPs and estate agents; the Companies legislation in both sides of the union which requires companies to keep beneficial ownership information; and the regulations on the declaration/disclosure regime for the cross-border currency and bear Negotiable Instruments (CBNIs) will also help strengthen the prevention of TF.

Meanwhile, additional measures will continue to be undertaken to guard against the risk of companies being abused for TF or PF purposes. Among other things, regulators are expected to conduct more AML/CFT/CPF joint on-site inspections on companies in URT or thematic inspection team on companies or firms which have a higher risk of being abused, based on relevant intelligence support and risk analysis.

LEAs will follow-up actions on companies which are found to be in breach of law. Through outreaching efforts of various forms such as circular letters, seminars and site inspections, TCSPs will be alerted to UNSC sanctions against sanctioned jurisdictions and reporting persons will be reminded of the requirements under the AMLA and AMLPOCA which demand risk-based approach, risk assessment of businesses and Submission STR/SAR.

Coupled with ongoing efforts to monitor and mitigate risk of FIs and DNFBPs the above initiatives will ensure the resilience and responsiveness of the CFT regime in URT. The Government will continue to monitor closely the terrorism threat and TF risk in URT, the effectiveness of the various counter-measures, and adjust the put in place a counter terrorism and CFT strategy as appropriate having regard to the changing security landscape and risk factors.

CONCLUSION

The 2022- 2027 Revised NRA demonstrates that criminals continue to use a wide range of money laundering techniques, including traditional ones, to move and conceal illicit proceeds depending on what is available or convenient to them. The findings show that new programs, products, and

technology will be exploited in future for fraud and laundering purposes as money launderers also adapt to changes and developments in the payments landscape. Key factors, such as actual or perceived anonymity, lack of transparency, complicit actors, and weaknesses in law will continue to be fundamental vulnerabilities that facilitate money laundering, TF and PF in URT.

The COVID-19 pandemic impact clearly had an effect in other jurisdictions and criminals exploited new avenues to generate and move illicit funds. Future assessments will look at these factors as a matter of post pandemic, and whether they mutated in post pandemic environment.

The new features in this Assessment that were not addressed in previous NRA, should provide greater awareness raising and more insight to the public and private sector stakeholders and should aid with understanding and managing risks. There is a need to ensure that sectoral risks and individual reporting persons undertake their own risks assessment drawing guidance from the identified threats, vulnerabilities and Risks in this 2022 NRA. As such, the findings of this report are expected to help develop policy responses to mitigate the money laundering risks identified, mainly through the issuance of the 2022/23-2026/27 Strategy.

LIST OF ACRONYMS

AML - Anti-Money Laundering
AMLA - Anti-Money Laundering Act (For Tanzania Mainland)
AMLPOCA - Anti-Money Laundering and Proceeds of Crime Act (For Zanzibar)
ATI - Association of Tanzania Insurers
BOT - Bank of Tanzania
BPRA - Zanzibar Business and Property Registration Agency
BRELA - Business Registration and Licensing Agency
CBDC - Cross Border Declaration of Currency
CDD - Customer Due Diligence
CIS - Collective Investment Scheme
MSA - Capital Markets and Securities Authority
CNCDC - Commission for National Coordination and Drug Control
CTR - Cash Transaction Report
DCC - Drugs Control Commission
DNFBPs - Designated Non-Financial Services Businesses and Professions
DSE - Dar es salaam Stock Exchange
EAC - East African Community
EFTR - Electronic Funds Transfer Report
ESAAMLG - Eastern and Southern Africa Anti-Money Laundering Group
EWURA - Energy and Water Utilities Regulatory Authority
FATF - Financial Action Task Force
FI - Financial Inclusion
FIU - Financial Intelligence Unit
FT - Financing of Terrorism
FP – Financing of Proliferation
GBT - Gaming Board of Tanzania
GDP - Gross Domestic Product
KYC - Know Your Customer
LEA - Law Enforcement Agency
LGA - Local Government Authority
ML - Money Laundering
MNO - Mobile Network Operator
MVTS - Money or Value Transfer Services

NAMLC - National Multi-Disciplinary Committee on Anti-Money Laundering
NBAA - National Board of Accountants and Auditors
NBS - National Bureau of Statistics
NCTC - National Counter Terrorism Centre
NEC - National Electoral Commission
NGO - Non-Governmental Organization
NIDA - National Identification Authority
NOMADS - Nominated Advisors
NRA - National Money Laundering and Terrorist Financing Risk Assessment
NRAWG - National Risk Assessment Work Group
PCCB - Prevention and Combating of Corruption Bureau
PF – Proliferation Financing
POTA - Prevention of Terrorism Act, 2002
RBA - Risk Based Approach
RITA - Registration, Insolvency and Trusteeship Agency
ROSCAS - Rotating Savings and Credit Associations
SACA - Savings and Credit Association
SACCOS - Savings and Credit Cooperative Society
SADC - Southern Africa Development Community
SSRA - Social Security Regulatory Authority
TACBA - Tanzania Court Brokers Association
TANESCO - Tanzania Electric Supply Company Limited
TBA - Tanzania Bankers Association
TBML - Trade Based Money Laundering
TCRA - Tanzania Communications Regulatory authority
TF - Terrorist Financing
TIC - Tanzania Investment Centre
TIN - Taxpayer Identification Number
TIRA - Tanzania Insurance Regulatory Authority TLS - Tanganyika Law Society
TMX - Tanzania Mercantile Exchange
TPF - Tanzania Police Force
TRA - Tanzania Revenue Authority
TZS - Tanzania Shillings (currency of the United Republic of Tanzania)
URT - United Republic of Tanzania

US - United States of America)
VSLA - Village Savings and Loans Association WB - World Bank
ZAAA - Zanzibar Association of Accountants and Auditors
ZAECA - Zanzibar Anti-Corruption and Economic Crimes Authority
ZAWA - Zanzibar Water Authority
ZEC - Zanzibar Electoral Commission
ZIPA - Zanzibar Investment Promotion Authority
ZLS - Zanzibar Law Society ZRB - Zanzibar Revenue Board