P O Box 427 Pretoria 0001 South Africa
370 Helen Joseph Street Pretoria 0002
+27 12 313 3911 / 0861 12 7272
www.resbank.co.za

South African Reserve Bank
Prudential Authority

Ref.: 15/8/2

G4/2023

To: All banks, controlling companies, branches of foreign institutions, eligible institutions and auditors of banks or controlling companies

Guidance Note issued in terms of section 6(5) of the Banks Act 94 of 1990

Guidelines for matters related to the prevention of banks or controlling companies being used for terrorist financing or other related unlawful activity

Executive summary

The purpose of this guidance note is to provide guidance to banks, controlling companies, branches of foreign institutions, eligible institutions and auditors of banks or controlling companies in respect of matters concerning adequate counter-financing of terrorism (CFT) controls.

Section 64A of the Banks Act, 1990 (Act No. 94 of 1990) read with regulations 39, 36(17) and 50 of the Regulations relating to Banks (Regulations) require every bank and every controlling company, among others, to have in place board approved policies and comprehensive risk-management processes and procedures, which policies, processes and procedures include comprehensive and robust know-your-customer standards that inter alia include robust customer identification, verification and acceptance requirements throughout the banking group, contribute to the safety and soundness of the reporting bank or controlling company, and prevent the bank or controlling company or other relevant entities within the group from being used for terrorist financing (TF) or other related unlawful activity.

Furthermore, regulation 36(17) of the Regulations requires, among others, that the aforementioned policies, processes and procedures must be sufficiently robust and ensure that the bank or controlling company inter alia continuously receives relevant information relating to risk exposure incurred by any foreign operation and that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies anti-money laundering (AML)/CFT measures consistent with the relevant Financial Action Task Force (FATF) Recommendations issued from time to time; the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.

1. Introduction

1.1. The FATF in its International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (FATF Standards) outlines the international standards which all countries ought to prescribe to. The FATF

Standards were updated in February 2023. Within South Africa, the legislation which seeks to support the FATF Standards are the Financial Intelligence Centre Act, 2001 (Act No. 28 of 2001) (FIC Act) and the Protection of Constitutional Democracy Against Terrorism and Related Activities Amendment Act, 2004 (Act No. 33 of 2004[1]) (POCDATARA Act).

1.2. Recommendation 6 of the FATF Standards requires each country to implement targeted financial sanctions (TFS) related to terrorism and terrorist financing to comply with the United Nations Security Council resolutions (UNSCR) that require countries to freeze, without delay, the funds or other assets, and to ensure that no funds and other assets are made available to or for the benefit of: (i) any person[2]or entity designated by the United Nations Security Council (the Security Council) under Chapter VII of the Charter of the United Nations, as required by UNSCR 1267 (1999) and its successor resolutions[3]; or (ii) any person or entity designated by that country pursuant to UNSCR 1373 (2001).

1.3. Recommendation 16 of the FATF Standards requires that countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain. Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information and take appropriate measures. Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant UNSCRs, such as UNSCR 1267 (1999) and its successor resolutions, as well as UNSCR 1373 (2001) relating to the prevention and suppression of terrorism and terrorist financing.

1.4. Recommendation 18 of the FATF Standards requires financial institutions to implement programmes against money laundering (ML) and TF. Financial groups should be required to implement group-wide programmes against ML/TF, including policies and procedures for sharing information within the group for AML/CFT purposes. Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML/CFT measures consistent with the home country requirements implementing the FATF Recommendations through the financial groups' programmes against ML/TF.

1.5. Recommendation 19 requires financial institutions to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks. Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

[1] Amended by Act No. 33 of 2022
[2] Natural or legal person
[3] Recommendation 6 is applicable to all current and future successor resolutions to resolution 1267 (1999) and any future UNSCRs which imposed targeted financial sanctions in the terrorist financing context.

1.6. Recommendation 20 states that if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).

1.7. Regulation 38(4) of the Regulations states, among others; when the Prudential Authority (PA) is of the opinion that a bank's policies, processes and procedures relating to its risk assessment or internal control systems are inadequate, the PA may require the bank, among others-

> *"to strengthen the bank's risk management policies, processes or procedures; or to strengthen the bank's internal control systems."*

1.8. This guidance note serves to inform and assist banks with information concerning CFT, as well as to understand the trends and typologies which may impact banks and controlling companies within South Africa.

1.9. The definitions as contained in Annexure A hereto are important to bear in mind when considering this guidance note:

2. Legislation in South Africa

2.1. Section 42(1) of the FIC Act stipulates that an accountable institution must develop, document, maintain and implement a programme for AML/CFT and proliferation financing risk management and compliance.

2.2. Regulation 36(17) of the Regulations requires, among others, that the policies, processes and procedures must be sufficiently robust and ensure that the bank or controlling company inter alia continuously receives relevant information relating to risk exposure incurred by any foreign operation and that every relevant foreign branch, subsidiary or operation of the bank or controlling company implements and applies AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time; the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host country are applied by the bank or controlling company.

2.3. Section 26A of the FIC Act states that *"A resolution adopted by the Security Council of the United Nations when acting under Chapter VII of the Charter of the United Nations, providing for financial sanctions which entail the identification of persons or entities against whom member states of the United Nations must take the actions specified in the resolution, has immediate effect for the purposes of this Act upon its adoption by the Security Council of the United Nations"*[4].

2.4. Section 23 of POCDATARA Act was amended[5] in 2022 to cover funds or other assets of persons and entities "*acting on behalf of, or at the direction of, or otherwise associated with a designated person*". The Financial Intelligence Centre (FIC) will issue notices on its website of freezing orders under section 23 of the

4 Read with Section 26B and 26C of the FIC Act

5 The FIC Act was amended in December 2022 to establish freezing obligations in respect of UNSCR obligations relating to UNSCR 1373 (2001) as well as persons and entities that are associated with the Taliban, Al-Qaida or ISIL (Da'esh) pursuant to UNSC Resolutions 1267 (1999), 1988 (2011), 1989 (2011) and 2253 (2015) obligations

POCDATARA Act (pursuant to UNSCR 1373), in accordance with section 3(1)(c) of the FIC Act which makes it an objective of the FIC to implement financial sanctions flowing from the UNSCR.

2.5. The FIC has also made available guidance, public compliance communications (PCCs) and the lists on its website, as well as the ability to subscribe for receipt of notifications if there are changes to the aforementioned lists. These are available at https://www.fic.gov.za/targeted-financial-sanctions/.

2.6. Section 24 and the Schedule to the POCDATARA Act made consequential amendments to the FIC Act to incorporate the implementation of TFS pursuant to UNSCRs 1267 (1999), 1989 (2011) and 1988 (2011) in the TFS mechanism provided for in sections 26A to 26C of the FIC Act. As a result, the mechanism that is used for the implementation of TFS under all other UNSCRs is now also used for TFS under UNSCRs 1267 (1999), 1989 (2011) and 1988 (2011).

3. Identification and assessment of TF risk

3.1. Banks should ensure that they clearly understand the TF risk exposure of their institutions and that they have a comprehensive risk management and compliance programme[6] (RMCP) to ensure compliance with their obligations in terms of the FIC Act.

3.2. This can be achieved through conducting comprehensive institution-wide TF risk assessments which clearly caters for the identification and assessment of its TF risks, which in turn informs the degree and extent of controls required to mitigate the risk posed to the bank concerned.

3.3. For the TF risk assessment exercise, the methodology utilised is critically important and requires that there is in depth coverage and analysis of three aspects of TF risks, i.e. threats, vulnerabilities and consequences.

3.4. It is important that the methodology documented is such that it prescribes there be adequate collection of data in respect of TF threats, vulnerabilities, and consequences that will enable the analysis for these three respective concepts.

3.5. Information could be obtained through an array of sources, including utilising publicly available information on the magnitude of terrorist financing, taking into account authorities' perceptions of the threats, vulnerabilities and consequences[7]. Some useful sources include guidance issued by the Wolfsberg Group[8], taking into account the Basel Core Principles[9] and Basel Committee on Banking Supervision (BCBS) guidelines, the FATF guidance[10], as well as information released by the Institute for Security Studies[11] and the Royal United Services Institute[12].

[6] Section 42 of the FIC Act 38 of 2001

[7] Countering the Financing of Terrorism: Good Practices to Enhance Effectiveness: https://www.imf.org/en/Publications/Books/Issues/2023/05/12/Countering-the-Financing-of-Terrorism-Good-Practices-to-Enhance- Effectiveness-515493

[8] https://wolfsberg-group.org/

[9] https://www.bis.org/publ/bcbs230.htm

[10] https://www.fatf-gafi.org/en/home.html

[11] https://issafrica.org/

[12] https://www.rusi.org/

3.6. Information pertaining to TF revealed through sector risk assessments and national risk assessments is also a useful source of information to consider.

3.7. The institution-wide TF risk assessment must utilise accurate and current data and must take into account the context of the bank, i.e. factors such as the size of the institution, customer base, product and service offerings, exposure to different business activities (e.g. trade finance services, correspondent banking etc.), country/geographical exposure, delivery channels, business operation complexity, transactional and operational TF risk.

3.8. The institution-wide TF risk assessment must enable banks to clearly understand the key threats and vulnerabilities to which the bank is exposed, as well as the degree to which the respective control measures in place mitigate such risks. Through the outcomes of the institution-wide TF risk assessment, the RMCP must document the processes and procedures linked to the TF control measures with clear identification of the resources allocated for the successful implementation and management of such controls, and these must be appropriate to mitigate the level of TF risk exposure. The processes and procedures must also ensure that there are adequate and prompt updates to the TF screening and alerts systems, transaction monitoring systems, manual detection mechanisms and payment screening systems.

3.9. Furthermore, the frequency of the risk assessments must also be documented in the RMCP and the RMCP should enable the bank to apply an agile approach in terms of emerging threat/vulnerability considerations.

3.10. Regular updates pertaining to TF should be applied to the RMCP, inclusive of triggers which prompt updates such as new product offerings, new client types, new geographic locations, delivery channels etc.

4. Mitigation of TF Risks

The following areas, when given sufficient attention, aid in mitigating TF risk:

4.1. Customer Due Diligence

4.1.1. Ensuring that there are sufficient onboarding processes to determine if potential clients pose a high risk of TF;

4.1.2. ensuring that the onboarding processes are sufficient to take into account TF risk exposure e.g. onboarding clients that frequently export goods to countries where TF threats are high;

4.1.3. maintaining accurate, complete and up to date client and transactional data;

4.1.4. conducting enhanced customer due diligence processes for high-risk clients or clients located in high-risk jurisdictions;

4.1.5. ensuring that adequate due diligence is performed in respect of banks where banking relationships are held, with sufficient attention being given to TF risk and mitigating controls in place by the correspondent bank;

4.1.6. existing clients must on an ongoing basis be assessed to determine if they pose new or the same level of TF risk;

4.1.7. beneficial owners of clients should be sanctioned screened, and the outcome of the screening should inform the overall TF risk appreciation of the client;

4.1.8. where beneficial owners are deemed to be high risk from a TF risk exposure

perspective, enhanced due diligence undertaken will assist in managing the overall risk associated with the client; and

4.1.9. processes for the exiting of clients should be properly documented, considering legislative requirements.

4.2. **Transaction monitoring**

4.2.1. Ensuring that transaction monitoring detection mechanisms can identify potential TF activity;

4.2.2. adequate procedures and processes are in place for identifying suspicious activity and reporting suspicious transactions linked to TF; and

4.2.3. keeping abreast of TF trends and typologies which may impact the TF risk assessment of a bank and inform new effective transaction monitoring rules or scenario detection mechanisms.

4.3. **Payment screening**

4.4. Implementing internal TF watchlists to screen persons or groups suspected of being linked to TF or persons who are high risk due to their participation in high-risk activity which involves links to TF activity;

4.4.1. maintaining internal watchlists and noting any domestic designations or cases which may involve bank clients or the beneficiaries of the transactions; and

4.4.2. the implementation of adequate freezing mechanisms to ensure compliance with the requirements of the FIC Act.

4.5. **Audit**

4.5.1. The execution of regular internal assurance and compliance reviews can assist with ascertaining if there is proper implementation of TF risk control measures undertaken by front-line/business functions; and

4.5.2. planned activities by internal and external audit should reflect testing of the adequacy of TF risk assessments and correlating controls on an ongoing basis, and the outcome of the audits should be communicated to senior management.

4.6. **Training**

4.6.1. General TF training should be provided to staff, as well as specialised TF training, taking into account the staff most exposed to high TF risk business environments; and

4.6.2. keeping abreast of regulatory changes and the latest local and international TF developments, trends and typologies and communication of such updates to staff is important to ensure that the bank is up to date and aware of emerging TF threats or vulnerabilities.

4.7. **Resources**

4.7.1. Adequate human resources should be employed to ensure that the TF risk is adequately mitigated across the business of the bank, and that the assignment of resources be commensurate with where there is a greater concentration of TF risk; and

4.7.2. adequate technological resources should be utilised to assist the bank with the implementation of TF risk mitigation measures, e.g. on TF risk mitigation it is important to ensure that adequate and effective controls are utilised to mitigate the

TF risk of a bank or banks within a banking group.

4.8. Governance and oversight

4.8.1. Adequate governance and oversight measures assist in ensuring that there is sufficient attention given to the mitigation of TF risk across banks and banking groups;

4.8.2. governance committees which enable reporting on the effectiveness of TF mitigating controls contribute to effective communication to senior management on key risk areas, including TF risk; and

4.8.3. the detail reported on should include pertinent statistical data and key risk indicators on the effectiveness of TF risk mitigation measures to enable senior management to appreciate the risks and be well positioned to escalate further action where required.

5. Mitigation of TFS Risks

The following areas, when given sufficient attention, aid in mitigating TFS risk:

5.1. Customer Due Diligence

5.1.1. Ensuring that there are sufficient onboarding processes to identify potential clients who may be designated by, or under the authority of, the Security Council under Chapter VII of the Charter of the United Nations, including: (i) in accordance with UNSCR 1267 (1999) and its successor resolutions; or (ii) designated by that country pursuant to UNSCR 1373 (2001);

5.1.2. ensuring that the onboarding processes are sufficient to take into account TFS risk exposure e.g. onboarding clients that frequently export goods to countries where the risk of engaging with persons who are subjects of TFS are higher;

5.1.3. maintaining accurate, complete and up to date client and transactional data so that screening can be a seamless and effective process;

5.1.4. conducting enhanced customer due diligence processes for clients who may be linked to such designated persons;

5.1.5. where beneficial owners are deemed to be high risk from a sanctions risk perspective, enhanced due diligence undertaken will assist in managing the overall risk associated with the client; and

5.1.6. processes for the exiting of clients should be properly documented, considering legislative requirements.

5.2. Transaction monitoring

5.2.1. Ensuring that transaction monitoring detection mechanisms can identify when designated persons have engaged in transactions or suspicious activity or attempted to bypass screening detection;

5.2.2. adequate procedures and processes are in place for identifying suspicious activity and reporting suspicious transactions; and

5.2.3. keeping abreast of TFS updates which may impact the risk assessment of a bank and inform new effective transaction monitoring rules or scenario detection mechanisms.

5.3. **Payment screening**

5.3.1. Efficient and effective payment screening mechanisms will serve to prevent payments to or from sanctioned individuals;

5.3.2. good practice includes ensuring that the correspondent bank's TFS screening tools are effective and calibrated to detect designated persons through name screening[13]and reference screening[14], including fuzzy matching[15] capabilities;

5.3.3. existing clients must be regularly screened against the requisite sanctions lists[16];

5.3.4. beneficial owners of clients should be sanctioned screened, and the outcome of the screening should inform the overall ML/TF risk appreciation of the client and freezing of assets should occur in the event that the beneficial owner is an individual;

5.3.5. ensuring that where UNSCR lists are provided by vendors, the lists are updated within 24 hours;

5.3.6. regular review of payment screening rules to ensure that they are relevant, effective, and comprehensive;

5.4. implementing internal TFS watchlists to screen persons or groups suspected of being linked to designated persons;

5.4.1. maintaining internal watchlists and noting any domestic sanctions designations or clients that could be linked to designated persons; and

5.4.2. the implementation of adequate freezing mechanisms ensure compliance with the requirements of the FIC Act.

5.5. **Audit**

5.5.1. Regular internal assurance and compliance reviews are conducted to ensure proper implementation of TF and TFS risk control measures undertaken by front-line functions; and

5.5.2. planned activities of internal and external audit should reflect testing of the adequacy of TF/TFS risk mitigation controls on an ongoing basis and ensure that the outcome of the audits is communicated to senior management.

5.6. **Training**

5.6.1. General TFS awareness training should be provided to staff, as well as specialised TFS training, taking into account the staff most often required to deal with such matters, for example payment screening or transaction monitoring staff, staff engaged in client assessments where enhanced due diligence is undertaken for clients in high-risk areas etc.; and

5.6.2. keeping abreast of regulatory changes and the latest local and international TFS lists, and ensuring the business is adequately trained on how to deal with instances where alerts are generated in respect of TFS and what reporting actions are required is important.

5.7. **Resources**

5.7.1. Adequate human resources should be employed to ensure that the TFS risk is adequately mitigated across the business of the bank, and that the assignment of resources be commensurate with where there is a greater concentration of TFS risk;

13 Screening of individuals, businesses, and counterparties against global sanctions lists
14 Screening strategy that allows you to check for potential matches in banking payment reference texts
15 This logic which uses algorithms to compare the similarity between two names based on their spelling, phonetics, and other factors
16 As per para 5.1.1

and

5.7.2. adequate technological resources should be utilised to assist the bank with the implementation of ongoing maintenance of TFS risk mitigation measures.

5.8. **Governance and oversight**

5.8.1. Adequate governance and oversight measures assist in ensuring that there is sufficient attention given to the mitigation of TFS risk across banks and banking groups;

5.8.2. governance committees which enable reporting on the effectiveness of TFS mitigating controls contribute to effective communication to senior management on key risk areas, including TFS risk; and

5.8.3. the detail reported on should include pertinent statistical data and key risk indicators on the effectiveness of TFS risk mitigation measures to enable senior management to appreciate the risks and be well positioned to instruct and prioritise further action where required.

6. Group wide implementation

6.1. Regulation 36(17) of the Regulations specifically requires that every relevant foreign branch, subsidiary or operation of the bank or controlling company apply AML/CFT measures consistent with the relevant FATF Recommendations issued from time to time, especially FATF Recommendation 18; the higher of AML/CFT standards issued in the Republic of South Africa or the relevant host should be applied by the bank or controlling company.

6.2. Where such home country AML/CFT standards cannot be implemented in a host country, the Chief Executive Officer of the relevant bank or controlling company should inform the PA accordingly, in writing.

6.3. The BCBS guidelines highlight that group policies and procedures should be designed to also identify, monitor and mitigate group-wide risks in addition to compliance with relevant laws and regulations. This includes TF risks and each host country should also have in place customised TF risk assessments which take into account idiosyncratic risks that may differ to that of the home country.

6.4. Section 42 of the FIC Act specifically requires that a bank's RMCP provide for the manner in which it is implemented in branches, subsidiaries or other operations of the institution in foreign countries.

6.5. Section 42 of the FIC Act also provides for the additional obligation for accountable institutions to provide for the manner in which the accountable institutions will apply appropriate additional measures to manage the risks if the host country does not permit the implementation of measures required in terms of the FIC Act.

7. TF General Concepts

7.1. The terrorism financing process typically involves four stages namely raising, storing, moving and utilisation of funds and other assets in support of terrorism. The stages are not necessarily sequential or linked to a specific terrorism related activity. These stages are detailed as follows:

7.1.1. Raising funds via numerous methods including legitimate means donations, not for profit organisations, self-funding, and criminal activity etc.;

7.1.2. storing funds intended for an individual terrorist or a terrorist group, network or cell by similar means used in moving funds while planning for their use;

7.1.3. moving funds to an individual terrorist or a terrorist group, network or cell through a series of witting or unwitting facilitators and/or intermediaries by means of banking and remittance sectors, informal value transfer systems, bulk cash smuggling and crypto assets, and smuggling high value commodities such as oil, art, antiquities, agricultural products, precious metals and gems, as well as used vehicles; and

7.1.4. using funds for payment when needed to further the terrorist organisation, group, network or cell's goals, including living expenses, to purchase weapons or bombmaking equipment and/or to finance terrorism operations.

7.2. It is important to bear in mind that the cost of a terrorist attack, or facilitating the movements of cell members cannot be compared to the proceeds of crime as in the case of for example, drug cartels. The cost of components for an improvised explosive device (IED), the purchase of a knife, the rental of a vehicle, the purchase of a plane ticket or the purchase of airtime pale in comparison to the amounts you will see in the placement, layering and integration phases of ML.

8. Trends and Typologies

8.1. The following trends and typologies are important when trying to detect terrorism financing:

8.1.1. Cash couriers and cash smuggling by individuals travelling to high-risk jurisdictions[17] and conflict zones;

8.1.2. the use of the informal financial systems (e.g. Hawala[18]) by the émigré communities from countries associated with terrorism;

8.1.3. the use of the formal banking and money remittance services to send funds to high-risk jurisdictions and conflict zones. Not all transactions will be related to terrorism financing, making the identification of such transactions more complex;

8.1.4. the issuing of multiple debit/credit cards that are used simultaneously domestically and in high-risk jurisdictions would be regarded as a red flag.

8.1.5. the use of compromised immigration, refugee, and asylum documents, especially by members of the émigré community, which are then used to open bank accounts, register for money remittance services and open accounts with crypto asset service providers;

8.1.6. the use of bank accounts to register with crypto asset service providers (CASPs), funds are then transferred to virtual wallets associated with crowdfunding platforms linked to terrorist organisations;

8.1.7. the use of online or virtual payment systems to facilitate the purchase of goods,

[17] High risk and other monitored jurisdictions (fatif.gafi.org)
[18] The role of Hawala and other similar service providers in money laundering and terrorist financing (fatf-gafi.org)

remit funds, and the payment of utilities, that fall outside the scope of the formal banking transaction systems run the risk for been abused for terrorism financing; and

8.1.8. the not-for-profit sector, which includes Non-profit Organisations (NPO), Public Benefit Organisations as well as a company registered in terms of section 21 of the Companies Act, 1973 (Act No. 61 of 1973), run the risk of abuse by terrorist financiers, and can be used as a vehicle to raise, store and move funds.

8.2. Furthermore, the Non-Profit Organisations Act, 1997 (Act No. 71 of 1997) (NPO Act), as amended, introduced the following:

8.2.1. requiring registration of specified non-profit organisations in terms of the NPO Act;

8.2.2. enabling the NPO Directorate, in order to perform its functions, to collaborate, co-operate, co-ordinate and enter into arrangements with other organs of state;

8.2.3. clarifying the scope of powers of the director in relation to the registration and cancellation of registration of non-profit organisations, and in respect of the power to require amendments to be effected to the constitution of a NPO;

8.2.4. by requiring registered NPOs to submit prescribed information about the office-bearers, control structure, governance, management, administration and operations of NPOs to the director;

8.2.5. requiring prescribed information relating to the office-bearers, control structure, governance, management, administration and operations of registered NPOs to be included in the register that the director must keep, and by providing for access to that information;

8.2.6. by providing for grounds for disqualification for a person to be appointed or continuing to act as an office-bearer of a registered NPO;

8.2.7. by providing for the removal of an office-bearer; and

8.2.8. by providing for certain contraventions.

8.3. Ultimately it is important that banks understand the profile of the NPO entities that are banked and ascertain if the NPO through its services may be exposed to individuals who may abuse the NPO for the purpose of TF. This needs to be understood without interfering with the type of work/services they deliver. It may just be an individual within the NPO and not the entire NPO, the geographic location and where the NPO operates may make it more susceptible to abuse.

8.4. Organisations that operate near or in conflict zones, pose a higher risk for terrorism financing.

8.5. Terrorism financing and its nexus to organised crime include kidnapping for ransom, extortion, trafficking in firearms, dealing in precious metals, gold and counterfeit goods. These avenues are exploited to generate funds for terrorist organisations.

9. Acknowledgement of Receipt

9.1. Kindly ensure that a copy of this guidance note is made available to your institution's independent auditors. The attached acknowledgement of receipt, duly completed and signed by both the Chief Executive Officer of the institution and the said auditors, should be returned to the PA at the earliest convenience of the aforementioned signatories.

Fundi Tshazibana

Fundi Tshazibana
Chief Executive Officer

Date: 09/12/23