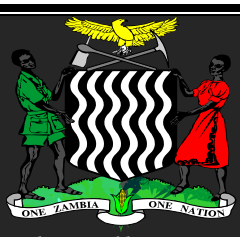

Financial Intelligence Centre
Republic of Zambia

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRRORISM GENERAL GUIDELINES, 2017

DECEMBER 2017

The Financial Intelligence Centre Act

(No. 46 of 2010)

Anti-Money Laundering and Combating the Financing of Terrorism General Guidelines, 2017

IN EXERCISE of the powers contained in *section fifty-six* of the Financial Intelligence Centre Act Number 46 of 2010, as amended by Act No. 4 of 2016) (hereinafter the FIC Act) the following Guidelines are hereby made:

Purpose

1. The Financial Intelligence Centre (the Centre) has issued these guidelines to clarify the regulatory expectations for implementing obligations imposed on a reporting entity to the extent that those obligations have not yet been clarified in other guidelines or regulations issued by the Centre.

2. It should be appreciated that the key underlying objective of these guidelines is to provide a reporting entity with guidance to enable it gain a demonstrable understanding of the nature and level of its money laundering (ML) and terrorist and proliferation financing (PF/TF) risks; develop and apply anti-money laundering/combating the financing of terrorism and proliferation (AML/CPF/CFT) policies (including group-wide policies), internal controls, and programmes to adequately mitigate those risks; apply appropriate customer due diligence measures to identify and verify their customers (including the beneficial owners) and conduct on-going monitoring; adequately detect and report suspicious transactions; and comply with the AML/CPF/CFT obligations imposed on them by the FIC Act.

Caveat

3. A reporting entity should take note that the contents of these Guidelines are neither intended to be, nor should they be construed as, an exhaustive list of the means by which a reporting entity can meet their legal and regulatory requirements contained in the FIC Act, 2010 and the regulations issued thereunder.

Guidelines

Risk Based Approach

4. *Regulation 8* of the Financial Intelligence Centre (General) Regulations, S.I No. 9 of 2016 (FIC General Regulations) requires a reporting entity to adapt the nature and extent of application of the customer due diligence measures commensurate with the level of the money laundering and terrorist financing risk associated with the customer, business relationship or transaction.

5. The risk-based approach to customer due diligence and on-going monitoring is recognized as an effective way to combat ML/TF. The general principle of a risk-based approach is that where customers are assessed to be of higher ML/TF risks, a reporting entity should take enhanced measures to manage and mitigate those risks, and that correspondingly where the risks are lower, simplified measures may be applied.

6. The use of a risk-based approach has the advantage of allowing resources to be allocated in the most efficient way directed in accordance with priorities so that the greatest risks receive the highest attention.

7. For example, the risk-based approach may require extensive customer due diligence for high risk customers, such as an individual (or corporate entity) whose source of wealth and funds is unclear or who requires the setting up of complex ownership and control structures.

8. A reporting entity should be able to demonstrate to a supervisory authority that the extent of customer due diligence and ongoing monitoring is appropriate in view of the customer's ML/TF risks.

9. There are no universally accepted methodologies that prescribe the nature and extent of a risk-based approach. However, as indicated in *Regulation* 13 of the FIC (General) Regulations, an effective risk-based approach does involve identifying and categorizing ML/TF risks at the customer level and establishing reasonable measures based on risks identified. An effective risk-based approach will allow a reporting entity to exercise reasonable business judgment with respect to its customers.

10. A risk-based approach should not be designed to prohibit a reporting entity from engaging in transactions with customers or establishing business relationships with potential customers, but rather it should assist it to effectively manage potential ML/TF risks associated with the customer.

Anonymous accounts and fictitious names

11. *Section 15* of the FIC Act prohibits a reporting entity from establishing an anonymous account or any account in a fictitious name. This obligation entails the following:

    a. That a reporting entity must not establish an account that does not bear a name.

    b. The name of an account must be a real name of the account holder

    c. An account should be broadly understood as including other similar business relationships between a reporting entity and its customers.

12. *Section 16(1)(b)* of the FIC Act, 2010 provides for a prescription of a transaction limit above which a financial institution must obtain and verify the identity of a customer who is neither an account holder nor in an established business relationship with the financial institution. *Regulation 5* of the Financial Intelligence (Prescribed Threshold) Regulations, S.I No. 56 of 2016 (herein after 'Prescribed Threshold) Regulations)), has clarified that there is no minimum amount of an occasional transaction below which A reporting entity may not conduct customer due diligence. Instead financial institutions are required to identify and verify the identity of any customer who wishes to carry out an occasional transaction in any amount. This should be applied within the context of *Regulation* 8 of the FIC (General) Regulations discussed in paragraph 14 below.

Other reliable and independent source documents for verification of customer identity

13. *Regulation 7* of the FIC (General) Regulations has prescribed other forms of reliable and independent source documents for the verification of customer identity. These include a reference from the individual's employer or a professional or customary authority that has known that individual for at least a year.

14. In line with *regulation 8* of the FIC (General) Regulations which allows a reporting entity to adapt the nature and extent of application of the customer due diligence measures commensurate with the level of the money laundering and terrorist financing risk associated with the customer, business relationship or transaction, a reporting entity should only consider use of other forms of verifying customer identity in cases of lower risk customers and or products as prescribed in the Second Schedule to the FIC (General) Regulations.

15. In all cases involving normal or higher risk customers and or products, a reporting entity must verify the identity of the customer using the individual's driving licence, passport or national identification document bearing the individual's pictorial image as provided for in *regulation 7* of the FIC (General) Regulations.

Circumstances for postponement of verification of customer identification

16. *Section 16(4)* of the FIC Act envisages circumstances in which the verification of customer identity may be postponed after the commencement of a business relationship.

17. Examples of situations where it may be necessary not to interrupt the normal conduct of business include:

    a. securities transactions – in the securities industry, companies and intermediaries may be required to perform transactions very rapidly, according to the market conditions at the time the customer is contacting them, and the performance of the transaction may be required before verification of identity is completed; and

    b. Life insurance business – the verification of the identity of the beneficiary under the policy may take place after the business relationship with the policy holder is established, but in all such cases, verification should occur at or before the time of pay-out or the time when the beneficiary intends to exercise vested rights under the policy.

18. In all such cases, as *Section 16(4)* of the FIC Act requires, the two conditions that must be satisfied are:

a. the risk of money laundering or financing of terrorism must be effectively managed; and

b. A delay in verification must be deemed essential not to interrupt the normal conduct of business.

19. Therefore, based on the foregoing, where a reporting entity permits its customer to utilise the business relationship prior to verification, the reporting entity should adopt appropriate risk management policies and procedures concerning the conditions under which this may occur. These policies and procedures should include:

a. establishing timeframes for the completion of the identity verification measures;

b. regular monitoring of such relationships pending completion of the identity verification, and keeping senior management periodically informed of any pending completion cases;

c. obtaining all other necessary customer due diligence information;

d. ensuring verification of identity is carried out as soon as it is reasonably practicable;

e. advising the customer of the obligation of a reporting entity, under *Section 21* of the FIC Act, to terminate the relationship at any time on the basis of non-completion of the verification measures;

f. placing appropriate limits on the number of transactions and type of transactions that can be undertaken pending verification; and

g. Ensuring that funds are not paid out to any third party. Exceptions may be made to allow payments to third parties subject to the following conditions:

i. there is no suspicion of ML/TF;

ii. the risk of ML/TF is assessed to be low;

iii. the transaction is approved by senior management, who should take account of the nature of the business of the customer before approving the transaction; and

iv. The names of recipients do not match with watch lists such as those for terrorist suspects and PEPs.

20. However, these exceptions do not apply to the life insurance sector.

Customer identification requirements

21. *Regulation 7* of the FIC (General) Regulations requires a reporting entity to verify the full name, date and place of birth, address and other particulars of the individual. In cases of low risk customers and or products as prescribed in the Second Schedule to the FIC (General) Regulations, A reporting entity may not require to verify the customer's address in line with *Regulation 8* of the FIC (General) Regulations, which allows a reporting entity to adapt the nature and extent of application of the customer due diligence measures commensurate with the level of the money laundering and terrorist financing risk associated with the customer, business relationship or transaction.

Identification of beneficial owner

22. *Section 16(6)* of the FIC Act requires a reporting entity to identify the beneficial owner and take such reasonable measures as are necessary to verify the identity of the beneficial owner.

23. In determining what constitutes reasonable measures to verify the identity of a beneficial owner and reasonable measures to understand the ownership and control structure of a legal person or trust, a reporting entity should consider and give due regard to the ML/TF risks posed by a particular customer and a particular business relationship.

24. In order to satisfy the requirement of *Section 16(6)* of the FIC Act, a reporting entity should establish and maintain customer due diligence procedures that are reasonably designed to identify and verify the identity of beneficial owners of an account, as appropriate, based on the institution's evaluation of risk pertaining to an account. For example, customer due diligence procedures may include the following:

a. Determining whether the customer is acting as an agent for or on behalf of another, and if so, obtaining information regarding the capacity in which and on whose behalf the customer is acting.

b. Where the customer is a legal entity whose shares are not publicly traded in Zambia, such as an unincorporated association, a private company, trust or foundation, obtaining information about the structure or ownership of the entity so as to allow a reporting entity to determine whether the account poses heightened risk.

c. Where the customer is a trustee, obtaining information about the trust structure to allow a reporting entity to establish a reasonable understanding of the trust structure and to determine the provider of funds and any persons or entities that have control over the funds or have the power to remove the trustees.

d. With respect to accounts that have been identified by the customer due diligence procedures of a reporting entity as posing a heightened risk, these accounts should be subjected to enhanced due diligence that is reasonably designed to enable compliance with the requirements of the FIC Act. This may include steps, in accordance with the level of risk presented, to identify and verify beneficial owners, to reasonably understand the sources and uses of funds in the account, and to reasonably understand the relationship between the customer and the beneficial owner.

e. Certain trusts and corporate entities are examples of customers that may pose heightened risk.

f. In addition, a reporting entity should use customer due diligence and enhanced due diligence information for monitoring purposes and to determine whether there are discrepancies between information obtained regarding the account's intended purpose and expected account activity and the actual sources of funds and uses of the account.

25. A reporting entity whose customer due diligence procedures fail or are likely to fail to fulfil the requirements to identify beneficial owners is prohibited under *Section 21* of the FIC Act from establishing an account for, or

maintaining the business relationship with, that customer, and must make a report to the Centre.

Determination of high risk customers

26. *Section 19(b)* of the FIC Act requires a reporting entity to have appropriate risk management systems to identify customers whose activities may pose a high risk of money laundering and financing of terrorism and exercise enhanced identification, verification and on-going due diligence procedures with respect to such customers.

27. Further, *regulation 12* of the FIC (General) Regulations provides factors that a reporting entity should take into account in determining whether or not a customer may pose a high risk of money laundering and financing of terrorism. Proper consideration of the said factors will assist a reporting entity to monitor higher-risk situations. These factors point to situations that present a higher money-laundering risk which might include, but are not restricted to:

    - customers linked to higher-risk countries or business sectors;
    - customers who have unnecessarily complex or opaque beneficial ownership structures
    - transactions that are unusual, lack an obvious economic or lawful purpose, are complex or large or might lend themselves to anonymity

28. The definition of 'high risk customers' provided in the FIC Act includes Politically Exposed Persons (PEPs). The FIC Guidance Note on Politically Exposed Persons provides more details on the legal obligations when a reporting entity is dealing with a PEP.

Automated Screening of Customers

29. *Regulation 12 (1)* of the FIC (General) Regulations requires a reporting entity to implement risk management systems to identify high risk customers whose activities may pose a high risk of money laundering and financing of terrorism including. In order to satisfy this requirement, a reporting entity may consider using automated processes for checking customers against publicly available sanctions and Politically Exposed Persons' listings.

Employee screening procedures

30. *Section 23(2)(b)* of FIC Act requires a reporting entity to develop and implement adequate screening procedures to ensure high standards when

hiring employees. In order to satisfy this requirement, a reporting entity should consider carrying out mandatory background screening of staff as part of the recruitment process. The information a reporting entity could consider collecting in order to satisfy itself with regard to the probity and integrity of its staff include the following:

a. The name of the employers where the staff previously worked;

b. The reasons the staff left their previous employment;

c. A declaration of no criminal history by the employee

d. Where applicable, certificate of good conduct and standing from professional body of the employee.

Employee training

31. *Section 23(2)(c)* of FIC Act, 2010 requires a reporting entity to develop and implement programmes for the prevention of money laundering, financing of terrorism and any other serious offence. Such programmes must include on-going training for officers and employees to make them aware of the laws relating to money laundering the financing of terrorism and any other serious offence, to assist them in recognising transactions and actions that may be linked to money laundering, financing of terrorism and any other serious offence and instruct them in the procedures to be followed in such cases.

32. In order to satisfy this legal requirement, a reporting entity should ensure that such programmes are able to keep employees informed of new developments, including information on current money laundering and financing of terrorism techniques, methods and trends and provision of explanation of all aspects of laws, regulations and other enforceable means for combating money laundering and terrorist financing. In particular, employees must be provided with adequate explanations regarding requirements concerning customer due diligence, identification of suspicious transactions and suspicious transaction reporting.

On-going due diligence

33. *Section 24* of the FIC Act requires a reporting entity to exercise on-going due diligence with respect to any business relationship with a customer.

34. For instance, the Second Schedule to the FIC (General) Regulations outlines factors to be considered in identifying higher risk customers, products and geographical locations. However, the identification of higher risk customers, products and services, including delivery channels, and geographical location is not a static assessment. These factors will change over time, depending on how circumstances develop, and how threats evolve. In addition, while a risk assessment should always be performed at the inception of a customer relationship, for some customers, a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making monitoring of customer transactions and ongoing reviews a fundamental component of a reasonably designed risk-based approach.

35. In order to satisfy the on-going due diligence requirement, a reporting entity should ensure that as part of its on-going due diligence, it should:

    a. scrutinise transactions undertaken throughout the course of a relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, and where necessary, the source of funds.

    b. Adjust its risk assessment of a particular customer from time to time or based upon information received from a competent authority, and review the extent of the customer due diligence and ongoing monitoring to be applied to the customer.

    c. Ensure that documents, data or information collected under the customer due diligence process is kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

36. A reporting entity should also keep its policies and procedures under regular review and assess that its risk mitigation procedures and controls are working effectively.

Record Keeping Requirements

37. *Section 22* of the FIC Act requires a reporting entity to maintain all the books and records with respect to its customers and transactions and their underlying information. *Regulations 12 and 13* of the FIC (General)

Regulations also require a reporting entity to assess the money laundering and terrorist financing risks associated with its customer.

38. In order to satisfy these requirements, a reporting entity should keep records and relevant documents of the risk assessment it conducts so that it can demonstrate to a supervisory authority, among others:

    a. how it assesses the customer's ML/TF risk; and

    b. The extent to which the customer due diligence and ongoing monitoring is appropriate based on that customer's ML/TF risk.

Measures for Transactions Emanating from High Risk Countries

39. *Section 25* of the FIC Act and *Regulation 14* of the FIC (General) Regulations require a reporting entity to manage money laundering and terrorist financing risk by implementing appropriate measures for business relations and transactions from countries that do not apply international standards for combating money laundering and terrorist financing.

40. In order for a reporting entity to know the countries that do not apply international standards for combating money laundering and terrorist financing, a reporting entity should regularly check the website of the Financial Action Task Force (FATF)[1] www.fatf-gafi.org which publishes countries that insufficiently comply with the international standards for combating money laundering and terrorist financing.

41. A reporting entity should adopt a balanced and common sense approach with regard to customers connected with countries that do not or insufficiently apply the FATF Recommendations. While extra care may well be justified in such cases, unless a supervisory authority or the Centre has, through a "notice in writing", imposed a general or specific requirement on a reporting entity, it is not a requirement that a reporting entity should refuse to do any business with such customers or automatically classify them as high risk and subject them to enhanced due diligence process. Rather, a reporting entity should weigh all the circumstances of the particular situation and assess whether there is a higher than normal risk of ML/TF.

[1] See Appendix 1 that explains what the Financial Action Task Force is

Currency Transaction Reporting

42. *Section 30* of the FIC Act and *Regulation 7* of the FIC (Prescribed Threshold) Regulations require a reporting entity to report to the Centre any currency transaction in an amount equal to or above the Kwacha equivalent of US$10,000, whether conducted as a single transaction or several transactions that appear to be linked. Currency is defined under section 2 of the FIC Act as '*the coin and paper money of the Republic, or of a foreign country, that is designated as legal tender or is customarily used and accepted as a medium of exchange.*'

43. A reporting entity may take the following factors into account in determining whether transactions are linked:

    a. Whether or not the transaction amounts are similar;

    b. Whether the amounts are payable from one or more sources over a short period to same recipient, intermediary, country or destination; and

    c. Whether a customer regularly transfers funds to one or more destinations

    d. The frequency of transactions

44. In determining whether the transactions are in fact linked, a reporting entity should consider the above factors against the timeframe within which the transactions are conducted.

Inapplicability of confidential information

45. *Section 32* of the FIC Act states that no secrecy or confidentiality provision in any other law shall prevent a reporting entity from fulfilling its obligations under the Act. In particular *Section 17(c)* and *Section 20(g)* of the FIC Act envisages that a reporting entity in the course of its business may be requested to share customer identification details with other reporting entities. In order for a reporting entity to satisfy the requirement of sharing customer identification information, the following elements of information constitute customer identification details:

    a. Customer name

    b. Customer permanent address

c. Customer contact details such as telephone and facsimile number and e-mail address

d. Date and place of birth of customer

e. The nationality of the customer

f. Occupation of the customer

g. Name of employer of a customer

h. Official customer identification number or other unique identifier contained in an unexpired official document that bears the pictorial image of the customer

i. Type of account and nature of business relationship the customer has with a A reporting entity

j. Signature of the customer

Treatment of Circulated Sanctions Listings-reference to NATC & local Regulations

46. The UN Security Council passed United Nations Security Council Resolution (UNSCR) 1373 (2001), which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UNSCRs regarding terrorism can be found at: www.un.org/Docs/sc/committees/1373/

47. The UN has also published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Osama bin Laden, Al-Qaida, and the Taliban under relevant UNSCRs (e.g. UNSCR 1267 (1999), 1390 (2002) and 1617 (2005)). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matched to the relevant authorities.

48. Based on the foregoing, a reporting entity is required to ensure that it does not maintain accounts or any business relationship with entities and individuals on the UN financial sanctions lists.

49. A supervisory authority circulates these UN Sanctions Lists to reporting entities from time to time with a request that a reporting entity responds indicating whether or not their customer data bases have names matching those of entities and individuals on the UN Sanctions Lists.

50. Every reporting entity is therefore expected to respond to such circulations to enable Zambia discharge its obligation to the UN in ensuring that those entities and individuals on the UN Sanctions Lists have no access to services or frozen assets in Zambia.

51. Where a reporting entity finds a positive match of names, this information must be communicated to a supervisory authority for further guidance in terms of specific follow up action that would be required of the reporting entity.

52. Considering that the UN Sanctions Lists are updated regularly, a reporting entity would do well to proactively check up with the UN website for the latest sanctions listings rather than to depend on the circulation of the list by a supervisory authority.

53. For an internationally active reporting entity, the UN Sanctions Listings are not the only ones that it must check. Other relevant sanctions lists that a reporting entity should regularly check include those of the United States of America (the Office of Foreign Assets Control list) and European Union.

54. In order for a reporting entity to be able to efficiently check all these various sanctions lists, it is recommended that a reporting entity automates its processes including the use of commercially available software tools.

Basis for Suspicious Transactions Reporting

55. *Notwithstanding that the sector specific STR guidelines provide detail on requirements on submission of STRs, reporting entities should have regard to Section 29* of the FIC Act which requires a reporting entity or its director, officer, or employee to submit a suspicious transaction report to the Centre under two circumstances:

    a. where it suspects or

    b. has reasonable grounds to suspect

that a predicate crime for money laundering may have been committed by a customer of the reporting entity.

56. "Suspects" is a subjective test. It requires employees of a reporting entity to report their suspicions without undue delay. Any employee who becomes suspicious (for example, a cashier accepting a large cash deposit or a clerk processing a large wire payment request) has an obligation to follow internal reporting procedures.

57. Employees who fail to report suspicious transactions under these circumstances are open to prosecution; Authorities only have to prove that the transaction was suspicious.

58. "Reasonable grounds to suspect" is an objective test. It places the onus on the employee to report circumstances where there are reasonable grounds for suspicion. Staff who do not file a report where there are reasonable grounds to be suspicious are at risk of prosecution by the authorities. The authorities need not prove that the employee was suspicious, only that there were reasonable grounds for suspicion.

Record Keeping on compliance measures by a reporting entity

59. A reporting entity should consider systematically collecting and maintaining information and statistics that support its compliance with its obligations to combat money laundering and terrorist financing under the FIC Act. Elements of information and statistics that must be collected and maintained include the following:

    a. frequency of internal AML/CFT compliance review; nature of breaches identified and remedial actions taken or sanctions applied;

    b. frequency and quality of AML/CFT training;

    c. time taken to provide competent authorities with accurate and complete customer due diligence information for AML/CFT purposes;

    d. Number of accounts/relationships rejected due to incomplete customer due diligence information;

    e. Number of wire transfers rejected due to insufficient requisite information).

f. number of STRs submitted, and the value of associated transactions;

g. number and proportion of STRs from different sectors; the types, nature and trends in STR filings corresponding to ML/TF risks;

h. Average time taken to analyse the suspicious transaction before filing an STR).

Other Factors for Demonstrating an understanding of money laundering and terrorist financing risks

60. Other factors that a reporting entity could consider in its efforts to gain a demonstrable understanding of the ML/TF risks include the following:

a. The type of measures implemented to identify and deal with higher (and where relevant, lower) risk customers, business relationships, transactions, products and countries;

b. Whether the manner in which AML/CFT measures are applied prevent the legitimate use of the formal financial system, and the type of measures taken to promote financial inclusion;

c. The extent to which the customer due diligence and enhanced or specific measures vary according to ML/TF risks across different sectors / types of institution, and individual institutions;

d. The extent to which a reporting entity relies on third parties for the customer due diligence process and how well it applies the controls;

e. The level of access to information that a reporting entity gives to its AML/CFT compliance function

f. The extent to which the internal policies and controls of a reporting entity enables timely review of: (i) complex or unusual transactions, (ii) potential STRs for reporting to the Centre, and (iii) potential false-positives

g. The extent to which the STRs submitted by a reporting entity to the Centre contains complete, accurate and adequate information relating to the suspicious transaction

h. The type of measures and tools a reporting entity employs to assess risk, formulate and review policy responses and institute appropriate risk mitigation and systems and controls for ML/TF risks

i. The manner in which a reporting entity communicates AML/CFT policies and controls to senior management and staff

j. The type of remedial actions and sanctions a reporting entity takes when it discovers that AML/CFT obligations have been breached

k. The manner in which a reporting entity documents its ML/TF risk assessments, and ensures that they are kept up to date; and

l. The adequacy of resources a reporting entity allocates to implementing AML/CFT policies and controls relative to its size, complexity, business activities and risk profile.

Other Sources of AML/CFT Guidance

61. The Financial Action Task Force has prepared a number of documents that provide detailed guidance to a reporting entity to assist them better implement their AML/CFT obligations under domestic legislation. Some of the guidance documents a reporting entity may consider consulting include the following:

    a. FATF Guidance for Financial Institutions in Detecting Terrorist Financing (2002)

http://www.fatf-gafi.org/media/fatf/documents/Guidance%20for%20financial%20institutions%20in%20detecting%20terrorist%20financing.pdf

    b. FATF Guidance on the Risk-Based Approach for the Banking Sector (2014)

http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

    c. Guidance for a Risk-Based Approach for Money or Value Transfer Services (2016)

http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-risk-based approach-money-value-transfer-services.pdf

d. Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services (2013)

http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-risk-based approach-NPPS.pdf

e. FATF Guidance on the Risk-Based Approach for the Life Insurance Sector (2009)

http://www.fatf-gafi.org/media/fatf/documents/reports/risk-based approach%20Guidance%20for%20Life%20Insurance%20Sector.pdf

f. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (February 2013)

http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

g. Guidance on Transparency and Beneficial Ownership (2014)

http://www.fatf-gafi.org/publications/fatfrecommendations/documents/transparency-and-beneficial-ownership.html

h. FATF Guidance Politically Exposed Persons (2013)

http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf

i. The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (2013)

http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-UNSCRS-Prolif-WMD.pdf

j. Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion (2013)

http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf

Appendix 1: The Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system. In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF Recommendations[2] set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

The FATF Recommendations have been endorsed by over 180 countries, and are universally recognised as the international standard for anti-money laundering and countering the financing of terrorism (AML/CFT).

Zambia is affiliated to FATF through its membership with the Eastern and Southern Anti-Money Laundering Group (ESAAMLG) which is a FATF observer member.

For more information or clarification, do not hesitate to contact the Centre at the address below:

The Financial Intelligence Centre
P. o. Box 30481
LUSAKA

Mary Chirwa Tshuma (Mrs)
Director General
Financial Intelligence Centre

November 2017

[2] The FATF Recommendations can be found on the FATF website www.fatf-gafi.org