Insurance Supervisory Institute of Mozambique (ISSM)

Notice No. 1 / CA-ISSM / 2019

Law No. 14/2013, of 12 August, and the respective regulation approved by Decree No. 66/2014, of 29 October, establishes the new regime for the Prevention and Combat of Money Laundering and the Financing of Terrorism in Republic of Mozambique, and among other things, it gives supervisory authorities the power to issue rules aimed at materializing compliance with the law.

If there is a need to guide the actions of financial institutions, which, under the terms of the referred law, are under its supervision, the Insurance Supervisory Institute of Mozambique, using the powers attributed to it by the combined provisions of Article 27 (b). Article 29 (2) (b) and (c) of the abovementioned Law provides:

1. The Insurance Sector Anti-Money Laundering and Counter-Terrorism Prevention and Fighting Guidelines, which are attached hereto, are hereby approved.
2. Failure to comply with the provisions of this notice constitutes a misdemeanor punishable under Law No. 14/2013 of 12 August.
3. This notice is effective 60 (sixty) days after its publication.
4. Any questions that may arise in the interpretation and application of this notice are clarified by the Directorate for Legal Affairs, Communication and Consumer Relations of the Insurance Supervisory Institute of Mozambique.
Maputo, 30 May 2019. - The Chairman of the Board of Directors, Maria Otília Monjane Santos.

Maputo, 30 May 2019. - The Chairman of the Board of Administration, Maria Otília Monjane Santos.

Guidelines on Preventing and Combating Money Laundering and Terrorist Financing Applicable to the Insurance Sector

Contextualization

Pursuant to Article 27 (b), in conjunction with Article 29 (2) (c), both of Law 14/2013 of 12 August Terrorist Financing - hereinafter the ML / TF Prevention and Fighting Act), which sets out the legal regime and measures to prevent and combat the use of the financial system and non-financial entities for the purpose of money laundering, terrorist financing and related crimes, it is the responsibility of the Insurance Supervisory Institute of Mozambique to issue general guidance to the By adopting these guidelines, it is intended to facilitate the implementation of measures to prevent and combat ML / TF and also the procedures to be verified in relation to clients, which should be adapted to the associated risk profile and considering the knowledge that the entity must have from its client.

These guidelines and guidelines are intended to:
a) Assist the players in the insurance sector in order to fully comply with their obligations under the BC / FT Prevention and Fighting Law and the respective regulation, approved by Decree No. 66/2014, of 29 October (Regulation of Law BC / FT Prevention and Fighting);
b) Interpret the requirements contained in the law and regulation as well as provide general guidance on their implementation; and
(c) assist insurance players in the implementation of the necessary preventive and control measures to mitigate the risk of their involvement in criminal practices.
These guidelines are addressed to entities operating in the insurance sector, which include:
a) Entities qualified to carry on the insurance business;
(b) pension fund management companies;
c) Insurance and reinsurance intermediaries;
d) Other related investment entities

CHAPTER I

Object and scope

1. These guidelines set out the procedures and measures to prevent and combat ML and TF.
2. These guidelines apply, under the terms of point c) of paragraph 2 of article 3 of Law no. 14/2013, of 12 August, to entities authorized to

carry on insurance, reinsurance, management companies supplementary pension funds, insurance and reinsurance intermediaries, and other related investment entities, hereinafter referred to as obligor entities.

CHAPTER II

Identification and verification duty

1. Obligated entities shall adopt policies on the identification and verification of their customers, in particular by defining the following elements:
a) Customer acceptance policy;
b) Customer identification and verification procedures;
c) monitoring of complex transactions; and
d) Risk management.
2. In formulating the customer acceptance policy, account shall be taken of the risks associated with the customers, and in particular the obliged entities shall evaluate the characteristics of the product requested, the purpose and nature of the business relationship and any other relevant factors, with the aim of creating and maintaining the risk profile of the policyholder relationship and identifying the type of customers, which is commonly known as KYC (know your customer).
3. The customer acceptance policy shall include in particular:
(a) the nature of the insurance policy which is liable to risk
money laundering and terrorist financing;
(b) the frequency and size of the activities;
(c) the history or profile of the customer and / or beneficial owner as
as a politically exposed person or linked to it;
d) The means, as well as the type of payments, cash, check or others;
e) the origin of funds;
(f) any other information that may suggest that the customer or beneficial owner is at high risk (eg. customer and / or beneficiary that has been refused by another obliged entity).

CHAPTER III

Customer Identification and Verification Procedures

SECTION I

General Procedures

In order to comply with the identification and verification obligations provided for in article 10 of Law no. 14/2013 of 12 August, the obliged entities, in relation to their clients, their representatives (other than their employees) and, if applicable, to other actors in operations, to adopt the procedures set out in the following subsections.

SUBSECTION I

Business relations

Whenever business relationships are proposed, either in person or at a distance, the obliged entities in relation to their clients (policyholders, underwriters or associates / participants) and, where appropriate, their representatives shall collect the identification elements required for policy issuance or pension fund management by extracting copies of the supporting documents, including:

1. Natural persons:
1.1. Information about:
a) Full name and signature;
b) Date of birth;
c) Place of birth and nationality;
d) Membership;
e) Sex;
f) Marital status and marriage regime;
g) Full address, namely the province, district, city, avenue or street and its number, or document proving the place of residence and telephone contact;
h) Letter from the employer certifying the employment relationship,
profession, type of contract, and net monthly salary;
(i) the type, number, place and date of issue of the identification document issued by the competent authority containing the current photograph of the holder, if applicable and within the validity period;
j) Unique Tax Identification Number - NUIT; and
(k) Nature and amount of income.

1.2. In order to prove the elements mentioned in

the previous number, the obliged entities must observe the following procedures:
(a) The identification elements referred to in points (a) to (d) shall be proved by:
I. Identity Card, in the case of national citizens;
II. Passport or DIRE for foreign citizens.
b) For minors who, due to their age, do not hold any of the documents referred to in the previous sub-paragraph, proof of their identification must be made by displaying the Birth Bulletin, or Birth Certificate, or , in the case of foreigners, from a public document equivalent to present by those who demonstrate that they are vested with the powers to legitimately contract, through documentary support considered suitable and sufficient by the obliged entities;
(c) the identification element referred to in point 1.1 (f). when not included in the document provided for in paragraph a) of this paragraph, it must be proved by the presentation of a Civil Registration Certificate or, in the case of foreigners, by means of an equivalent public document;
(d) The identification element referred to in point (g) shall be evidenced by any documentary support deemed appropriate and sufficient by the obliged entities, or by appropriate diligence to prove the stated address.
1.3. For foreign nationals, in the absence of unambiguous evidence of any or all of the above, obliged entities may request written confirmation of the truth and timeliness of the information provided by an insurer or a pension fund management company with which those citizens have a contract in force.
1.4. In remote operations, proof of information provided to obliged entities shall be provided by sending to the same entities, by registered mail, a certified copy of all supporting documentation of the required identification elements.
1.5. In the case of low risk clients, obliged entities may also prove the information provided by natural persons by means of accreditation by two witnesses of recognized suitability by the community or institution concerned, or by the comfort of the administrative entity responsible for the community.
2. Legal persons:
2.1. Information about:
(a) name or business name;
b) Headquarters, province, district, city, avenue or street in which it is located and its number and telephone contact;
c) Unique Tax Identification Number - NUIT;
d) Unique Number of Legal Entity;
e) Corporate purpose and purpose of the business;
f) Identity of qualified equity holders
Social;
(g) Economic Activity Classifier and Group Code economic, if applicable, issued by a licensing entity;
h) Identity of the holders of the governing bodies of the legal person and their mandate;
i) Specification of the powers of representation referred to in the previous sub-paragraph, which must be duly evidenced by authentic or authenticated documents, which unequivocally mention them, or in cases where such documents are not legally obtainable through private documents of equivalent content and legally binding;
j) Document issued by a competent entity authorizing the incorporation.
2.2. In the case of companies and other legal persons in
constitution, their identification shall include:
(a) full identification of the founding partners and other persons responsible for the company or other person to be incorporated, the requirements of paragraph 1 of this subsection being applicable;
b) Declaration of commitment to submit, within 90 days, the document of incorporation and proof of registration with the competent body.
2.3 In the case of individual establishments with limited liability or collective interests without legal personality, the arrangements provided for in paragraph 2 shall apply mutatis mutandis and beneficiary natural persons shall be identified in accordance with paragraph 1.
2.4. For the purpose of establishing the evidence referred to in paragraph 2.1.
obliged entities must observe the following procedures:
(a) The identification elements provided for in points (a) and (b) shall be demonstrated by the presentation of a Commercial Registration Certificate or other supporting public document;
b) The identification element provided for in subparagraph d) shall be evidenced by the presentation of a document issued by the Registry of Legal Entities or, in the case of foreigners, by an equivalent document;

(c) The particulars referred to in points (f) and (h) may be demonstrated by simple written declaration issued by the legal person itself containing the name or company name of the holders.
2.5. For foreign legal persons, in the absence of unambiguous evidence of any or all of the above, obliged entities shall adopt the procedure referred to in paragraph 1.3. this subsection.
2.6. In remote operations, the information provided to the obliged entities shall be verified in accordance with the provisions of paragraph 1.4.

SUBSECTION 2

Occasional Transactions

Whenever, in person or remotely, it is proposed to carry out occasional transactions the amount of which, alone or in combination, is equal to or greater than 450,000.00 MT, the obliged entities must observe, with the necessary adaptations:
(a) the identification requirements provided for in points (a) to (d) and (i) of paragraphs 1 and 2.2. and 2.3. Chapter III of these Guidelines;
(b) the means of proof provided, as appropriate, in paragraphs 1.2. to 1.4. or paragraphs 2.4. to 2.6. Chapter III of these guidelines.

SUBSECTION 3

Operations subject to special identification duties

1. Pursuant to Article 10 of Law No. 14/2013 of 12 August, obliged entities shall comply with the identification procedures provided for in paragraphs 1 and 2. and proof provided for in paragraphs 1.1. . to 1.3. or in paragraphs 2.1. a 2.3. as appropriate, whenever they propose to carry out an operation, in person or remotely and regardless of its amount, nature, and the entities involved, where it is likely that it may be related to the commission of the crime. money laundering and terrorist financing, provided for in Articles 4 and 5 of the ML / TF Prevention and Fighting Law, taking into account the specific characteristics of the transaction, namely its nature, complexity, atypical customer, amounts involved, frequency, economic situation of the actors or means of payment used.

2. For the purposes of these guidelines, when verifying transactions indicating the ML / TF, they constitute potentially suspicious transactions, other than those set out in paragraph 1.2. Annex 2 to the Regulation adopted by Decree 66/2014 of 29 October, as set out in Annex II to these guidelines.

SUBSECTION 4

Customer Due Diligence

1. General principle:
Customer Due Diligence Duty (CDD) is the central element of an effective ML / TF prevention and control program. It is the first and most important line of defense that obliged entities have to protect themselves from misuse of their activity to launder money or finance terrorism. CDD is a process, not a one-time event, as it begins with customer identification and continues throughout the life of the business relationship, as obliged entities are expected to follow the relationship and, if necessary, take all necessary steps to ensure that they know their client, as required by the ML / TF Prevention and Combat Act and the ML / TF Prevention and Combat Act Regulation.
1.1. Obligated entities should make every effort to determine the true identity of all customers requesting their services. There should be an explicit policy stating that transactions should not be conducted with customers who fail to provide proof of their identities.
1.2. Obligated entities shall refuse or terminate any transaction whenever the customer, his representative or beneficial owner, on request, refuses to provide the necessary elements to comply with the identification duties or, on the other hand, the risk assessment of the customer, customer or the transaction so requires.
2. Customer Due Diligence Measures:
2.1. Whenever there is any doubt as to the authenticity of the documents submitted or the veracity of the declaration made, the obliged entities should take the following steps:
a) Confirm the domicile at the addresses indicated, which may be by means of a trip to the place or by means of a declaration issued by the competent entity, or other elements deemed suitable;

b) Certify the authenticity of the documents displayed with
of the issuing entity;
c) To certify the legitimacy of the possession of funds presented, as well as their sources of income;
d) Send a suspicious transaction report to the Mozambique Financial Information Office (GIFiM).
2.2. Obligated entities may also obtain the information necessary to confirm the customer's identity by making use of available national and international public information, crosschecking information with other evidence and other steps they deem necessary.
2.3. Additional verification and due diligence measures that can be taken to ascertain the client's identity include the duty to identify and verify beneficial owners of legal persons by:
(a) identification of the natural or legal person holding 20 per cent or more of the company's share capital and voting rights;
(b) identification of members of the management bodies;
lawyers and their representatives;
c) Documents proving the information mentioned above, such as minutes, registration certificates or other documentation held by the entity.

SUBSECTION 5

Reinforced measures

Enhanced verification and due diligence measures should be applied to persons and entities presenting a higher risk to the institution. These measures may be applied when:
(a) a customer is not physically present to be identified;
b) The medium used by the client is complex and / or opaque, which makes
difficult to determine the identity of the beneficial owner;
c) The nature of a particular situation may represent a higher risk of ML / TF.

SUBSECTION 6

Politically Exposed People (PPE)

1. Without prejudice to the provisions of other legislation, obliged entities shall, in respect of PEPs, take the following measures:
(a) adopt appropriate risk management systems to determine whether or not a potential customer, an existing customer or the beneficial owner is an EPP;
(b) Develop a clear policy, appropriate internal control procedures and be especially vigilant regarding business relationships with PEPs, with persons and companies that are clearly related to or associated with them or other high risk customers.
2. Obligated entities shall take enhanced measures to determine the source of funds and resources of the client and beneficiaries identified as PPE. Financial institutions that have business relationships with clients in countries whose reputable public information portrays them as being vulnerable to corruption should identify PEPs in the country concerned and should seek to determine whether or not the client has family or business links with such persons.
3. Obligated entities shall carry out continuous monitoring, taking into account the fact that individuals may establish links with PEPs after the establishment of the business relationship.
4. Considering the fact that PEPs may not initially be identified as such, and whereas existing customers may subsequently acquire the status of PEPs, the institution shall regularly review its customers at least 12 (12 months.
5. Obligated entities should gather sufficient information about a new customer and verify the publicly available information to determine whether or not the customer is an EPP. An obliged entity, when considering establishing a relationship with a person suspected of being an EPP, must fully identify the EPP, as well as the persons and companies that are clearly related to it.

SUBSECTION 7

Simplified Measures

1. Obligated entities may apply simplified Customer Due Diligence measures when the customer is the State or a legal person governed by public law, of any nature, integrated into direct or indirect administration.
2. The insurance supervisory entity shall establish transactions which may lead to

simplified or reduced identification and verification measures, taking into account the nature and extent of the risk covered under non-life insurance, in accordance with the Group Recommendations. Financial Action Plan (FATF).
3. Simplified Customer Due Diligence measures shall not be applied when money laundering or terrorist financing is suspected or when the risks are highest.

CHAPTER IV

Transaction Monitoring

1. Obligated entities shall pay particular attention to all complex transactions, abnormally high value transactions and all unusual transactions of any other kind for which there is no apparent economic reason or visible legal purpose.
2. For the purposes of these guidelines, the term “transactions” refers, inter alia, to claims and proposals for insurance policy, premium payments, claims for benefit changes, beneficiaries and duration.

CHAPTER V

Risk management

1. Obligated entities shall identify, assess and understand the risks of ML / TF to the same obligated entities and take the necessary coordination measures in accordance with the risk assessment and shall apply resources to ensure that the same risks effectively mitigated.
2. For transactions made through new or developing technologies that favor anonymity, in particular via the internet or by mail, the obliged entity shall also apply effective customer identification procedures and continuously monitor observed customer standards. face to face.
3. In order to mitigate risks arising from non-face-to-face customers or from new technology transactions, the following measures may be applied:
(a) the certification by competent authorities of the identification documents submitted;
b) The request for additional documents to complement those required for face-to-face customers;
c) Direct contact with the client by the obliged entity;
(d) the presentation of a third party through a mediator who meets the criteria of the due diligence duty of the client;
(e) the claim for payment of insurance premiums through an account opened on behalf of the customer;
f) The most frequent and up-to-date information on non-face transaction clients.
4. Obligated entities shall adopt policies or take necessary measures to prevent misuse of technological developments in ML / TF schemes.

CHAPTER VI

Document Conservation

1. Identification documents, whether in physical, digital or microfilm form, shall, in accordance with Article 17 (1) to (4) of the ML / TF Prevention and Fighting Act, be kept for a period of 15 years. , from the date of termination of the business relationship.
2. Obligated entities shall, pursuant to Article 19 of the Rules of the BC / FT Prevention and Fighting Act, keep records resulting from Customer Due Diligence for a period of at least 15 years from the date of termination. business relationship, namely:
(a) copies of documents proving compliance with the
duty of identification and verification;
(b) a record of national and international transactions sufficient to permit the reconstitution of each operation to provide, where appropriate, evidence in criminal proceedings;
c) Justification of the decision not to communicate to GIFiM by the
Suspicious Operations Communication Officer.
3. This approach shall ensure that all customer and transaction records are available for consultation by law enforcement authorities with a view to preventing and combating ML / TF, as well as at the disposal of GIFiM when acting on exercise of its supervisory and inspection powers.
4. Obligated entities shall ensure that the duty to keep documents of operations as defined by law applies to branches, subsidiaries, agencies or

any other form of commercial representation located in the Mozambican territory with their headquarters abroad.
5. Retained documents shall be readily available to the ISSM upon request.

CHAPTER VII

Examination duty

1. Obligated entities shall:
a) Analyze with special care any transactions that may be related to the crime of money laundering, as defined in article 4 of Law 14/2013, taking into account, inter alia, their nature, complexity, unusual nature of the client's business, amounts involved, frequency, economic status of the actors or means of payment used;
b) Obtain written information on the origin and destination of the funds, the justification of the operations and the identity of the respective beneficiaries in relation to the operations provided for in the preceding paragraph and whose amount, individual or aggregate, is four hundred and fifty thousand meticals.
2. The assessment of the degree of suspicion evidenced by a given transaction stems not only from the existence of any type of documentation confirming the suspicions, but also and above all from a reasonable assessment of the concrete circumstances of the transaction.

CHAPTER VIII

Duty to collaborate

1. Obligated entities shall assist the competent judicial authorities, as well as GIFiM, upon request, by providing information on transactions carried out by their clients or by presenting documents relating to their transactions, assets or any other securities in their custody.
2. The request for cooperation from the judicial authorities shall be founded
in an ongoing criminal proceeding, duly individualized and
sufficiently achieved.

CHAPTER IX

Duty to abstain

1. Obligated entities shall refrain from performing operations that are reasonably suspected of constituting ML / TF crimes.
2. The obligated entities shall immediately inform the Public Prosecution Service and GIFiM that they have abstained from performing the operation under the terms of the previous number.

CHAPTER X

Internal control mechanisms and reporting suspicious transactions

SECTION I

Internal Control Mechanisms

1. Obligated entities shall designate, within their services, a person responsible for coordinating the internal control procedures in ML / TF matters and, in particular, for centralizing information on the facts provided for in Article 23 of Law no. 14/2013, of 12 August, as well as by communication to the competent authorities, in cases where it should take place.

2. Obligated entities shall have in place internal control mechanisms to ensure that the duties to which they are subject in the field of ML / TF are also observed at overseas branches and subsidiaries and shall expressly inform the ISSM where host country law prevent the application of principles and procedures appropriate to the performance of those duties.
3. Obligated entities shall develop ML / TF prevention programs that include at least:
(a) appropriate internal control policies, procedures and processes enabling the compliance, examination and risk assessment function, including:
I. Devices for monitoring operations, such as computerized systems for detecting and controlling higher-risk transactions;
II. Procedures to address the increased risk of money laundering and terrorist financing arising from the use of technologies that favor

anonymity.
(b) Appropriate procedures for hiring workers to ensure that they are carried out in accordance with strict ethical criteria.

SECTION II

Formation

1. Obligated entities shall ensure that their managers and employees are adequately trained in matters related to ML / TF prevention.
2. Obligated entities must have effective means to train their staff on all issues related to the ML / TF prevention and control regime.
3. Training programs shall keep employees up to date on ML / TF risk issues, all relevant laws and regulations, risk assessment, policies, procedures and internal control as set out in Article 42 of BC / FT Prevention and Combat.
4. Training shall be provided to all employees upon hiring by the obliged entity and shall be a permanent activity. In addition to general training, specific training programs should be developed for specific categories of staff depending on the nature of their role in ML / TF risk management. Records should be kept of the content of the training programs and the occasions on which they were conducted.

SECTION III

Suspicious Operations Communication Officer

1. The Board of Directors or similar body shall appoint to the head office, agencies, branches, branches and other forms of representation of the obliged entity, a Suspicious Transaction Reporting Officer (OCOS), chosen from management-level employees of the obligated entity. same entity.
2. The Management Board or similar body shall ensure sufficient resources for OCOS functionality, including human, material and technological resources.
3. Without prejudice to the provisions of other applicable legislation, the responsibilities of OCOS include:
(a) ensure that suspicious transaction reports are sent to GIFiM, with all relevant information;
(b) ensure the prompt forwarding of all additional information requested by the competent authorities in cases of suspected ML / TF cases;
c) Regularly review the adequacy of the system of controls on the prevention and control of ML / TF, including overseeing the implementation of policies and procedures for the prevention and combat of money laundering and terrorist financing;
Ensure that all relevant information on ML / TF prevention is passed on to workers, overseeing compliance with the institution's approved policies on training and ensuring that their content is appropriate, current and in line with good practice, practices and trends in the contours of the ML / TF phenomenon.

SECTION IV

Reporting Suspicious Operations

1. Obligated entities, during the monitoring process, should verify that the activity performed by the customer is consistent with their profile. In cases where the activity is inconsistent with the customer profile or for other reasons appears to be irregular or suspicious, obligated entities should investigate the relevant activities and transactions.
2. Pursuant to Article 18 of the BC / FT Prevention and Fighting Act, obliged entities shall report to GIFiM on transactions whose funds or assets are suspected to be related to the crime, or to be derived from the crime, or to be used for terrorist financing.
3. Obligated entities shall also notify GIFiM of all cash transactions of 250,000.00MT or more or any transfer of 750,000.00MT or more, in accordance with the BC / FT Prevention and Combat Act. .
4. In providing the information referred to in this section to GIFiM, obliged entities shall take all precautions to safeguard the necessary confidentiality, otherwise they may incur the commission of a crime typified under article 25 of the ML / TF Prevention and Combat Act. .
5. Reporting of suspicious information or transactions to GIFiM shall be based on current facts and shall be carried out immediately so as to permit its effective investigation.
6. Reporting to GIFiM shall as a minimum include:
(a) the identification, as complete as possible, of the persons involved in the transaction (eg borrowers / underwriters or beneficiaries) as well

as their activity;
(b) the characteristics of the transaction (eg total and partial amounts; time period covered; justification provided; currency used, suspicion indicators; means and payment instruments used).
7. Where it is decided not to notify the competent authorities, that decision shall be the subject of a reasoned opinion to be kept on file by the obliged entities for a period of at least five years.

CHAPTER XI

Final dispositions

1. Within the framework of business relationships already established at the date of the entry into force of this notice, obliged entities shall promote, based on materiality and risk weighted criteria, the updating of information relating to their customers in accordance with the identification and verification procedures provided for in this notice.
2. The provisions of this notice are without prejudice to or impaired by the application of other rules on the same matters issued by other financial system supervisors within the scope of their legal powers.

ANNEX I

Vulnerabilities in insurance business

1. Financial institutions, including insurers, have been the target of CB activities due to the variety of services and application instruments they provide which can be used to conceal the illicit origin of funds.
2. In fact, the insurance industry is vulnerable to ML / TF. When a life insurance policy expires or is redeemed, funds are made available to the policyholder or other beneficiaries. The beneficiary of the contract may be replaced prior to maturity or redemption for the purpose that payments may be made by the insurer to the new beneficiary. An insurance policy can be used as collateral to purchase other financial instruments.
3. Cash being an easily movable and fully replaceable instrument provides anonymity to many forms of criminal activity and the privileged means of exchange in the world of crime. This is due to the following:
a) Drug traffickers and criminals need
hide the true ownership and origin of the funds;
(b) also need to have control of the funds; and
c) In addition they must change the shape of the funds to cover their origins.
4. The most common form of ML / FT that insurers face is in the form of a proposal for a single premium policy. Examples of the type of contracts that are particularly attractive as vehicles for BC / FT are single premium applications, namely for:
(a) unit-linked contracts or non-unit-linked single premium contracts;
b) Purchase of annuities insurance;
(c) one-time deliveries of the value of an existing life insurance contract; and
(d) contributions at one time to retirement pension contracts.
These contracts alone may simply form part of a sophisticated web of complex transactions such as those described below and often originated elsewhere in the financial services sector.
6. BC / TF cases in non-life insurance may be seen in inflated or totally false claims, such as arson or other means causing a false claim to recover part of the legitimate funds invested.
7. Other examples include the cancellation of premium reversal policies by a check issued by the insurer, and the overpayment of premiums with a claim for overpayment. B / C can also occur through insurance, where a criminal can receive compensation for the full amount of damage, when in fact he should not.
8. Examples such as terrorist financing that can be facilitated through non-life insurance include the use of payments under occupational accident policies to support terrorists awaiting instructions to act, and primary coverage and commercial credit for transportation. materials to be used by terrorists.
9. BC / TF using reinsurance may occur either through the
establishment of fictitious reinsurers or reinsurance intermediaries, fronting schemes and captive reinsurers, either through the misuse of normal reinsurance operations. Examples include:
(a) the deliberate placement of proceeds of crime or terrorist funds by the insurer into

reinsurers for the purpose of disguising the origin of the funds;
(b) the establishment of fictitious reinsurers, which may be used to launder crime proceeds or to facilitate the financing of terrorists; and
c) The establishment of fictitious insurers, which may be used to place proceeds of crime or terrorist funds into legitimate reinsurers.
10. Insurance intermediaries are important for distribution, risk assessment and settlement of claims. They are often the direct link with the policyholder, and thus mediators should play an important role in preventing and combating ML / TF.
11. The same principles that apply to insurers should generally apply to insurance intermediaries. An individual wishing to launder money or finance terrorism may seek an insurance intermediary who is not informed or does not follow the necessary procedures, or who fails to recognize or report information regarding possible ML / TF cases. Mediators can themselves serve to channel illegitimate funds to insurers.

ANNEX II

Exemplary (specific) money laundering and terrorist financing indicators for the insurance sector

1. Single Premium Insurance Contracts:
(a) a request from a client to enter into an insurance contract (or more) where the origin of the funds is unclear and consistent with his or her standard of living;
(b) a proposal without any visible reason and a reluctance to justify the “need” to make the investment concerned;
(c) an offer to buy and settle a large amount of cash;
(d) an offer to purchase using a check drawn from a personal account other than that of the tenderer;
e) The prospective client does not wish to know the investment performance, but only questions about early cancellation / redemption of a specific type of contract;
f) The client who is presented by an overseas agent, subsidiary or other company is located in Non-Cooperating Countries and Territories (PTNC), designated regularly as FATF or in countries where drug production or trafficking may be predominant.
2. Insurer, workers and agents:
(a) unforeseen changes in worker characteristics, for example, a lavish lifestyle or avoiding vacation time;
(b) a sudden change in the performance of a worker or agent, for example, to record noteworthy performance or a noteworthy or unexpected increase in sales;
c) The use of an address other than that of the customer's permanent residence.
3. Other indicators using insurance contracts:
(a) early termination of a product, especially at a loss;
(b) a customer applying for an insurance policy concerning non-standard business activity;
(c) a client applying for an insurance policy in an amount considered beyond his apparent needs;
(d) a customer who attempts to use cash to complete a proposed transaction when such a transaction is normally made by check or other payment instrument;
e) A client who refuses, or does not wish to give, explanations about his financial activity, or gives explanations that are not true;
(f) a client who is reluctant to provide customary information when applying for an insurance policy, or who gives minimal or fictitious information, or who provides information that is difficult or expensive for the insurance institution to verify;
g) Delay in the delivery of information, which does not make it possible to complete the check;
h) A transfer of the benefit of a product to a third party with no apparent connection;
(i) replacement, during the life of an insurance contract, of the final beneficiary by a person with no apparent connection with the policyholder;
(j) an atypical incident of early payment of insurance premiums;
(k) insurance premiums were paid in one currency and the claim for compensation is made in another;
(l) any abnormal employment of an intermediary in the ordinary course of business or conventional activity, for example, the payment of compensation or high commission to an unusual intermediary;
m) A client who has policies with several insurers.

ANNEX III

GLOSSARY

Insurance policy: document that holds the contract between the policyholder and the insurer, containing the respective general, special (if any) and agreed particular conditions, depending on the conditions to be observed in their transfer.
Business risk assessment: This is an assessment that highlights a business's exposure to money laundering and terrorist financing risks and vulnerabilities, taking into account its size, nature and complexity and its customers, products and services, and the provision of these services.
Beneficiary: is the recipient of the benefit conferred by the obliged entity.
Beneficiary: Natural person (s) who actually owns or controls the customer and / or the person in whose name a transaction is made. It also includes those individuals who exercise effective control over a legal person or entity without legal personality.
Money laundering: It is characterized by a set of commercial or economic-financial operations with the objective of introducing into the financial system of a country, temporarily or permanently, resources, goods and values of illicit origin. Once these assets have been successfully laundered, the criminal can dispose of them without direct connection to their original source. In this order, the main purpose of money laundering is to legitimize income from illicit acts or business.
Client: the policyholder, understood as the natural or legal person who, on his or her behalf or on behalf of one or more persons, enters into the insurance contract with the insurer and is responsible for paying the premium. It also covers members, participants and beneficiaries.
Insurance contract: an agreement whereby the insurer or micro insurer undertakes, in return for the payment of a premium and in the event of the event to be covered, to be compensated, under the terms and within the agreed limits, damage caused to the insured or to the satisfaction of capital, income or other benefits provided for therein.
Identification data: data, documents, in whatever form, from a credible and independent source.
Customer Due Diligence - CDD) - stages in which an insurer is required to undertake in order to identify and verify the identity of the parties to a relationship and to obtain information on the intended purpose and nature of each business relationship.
Document: Information retained in any form (including, but not limited to, electronic form).
Terrorist Financing: The provision or collection of funds by any means, directly or indirectly, with the intention of using them, or knowing that they will be used, in whole or in part, to commit terrorist acts. For terrorists, raising funds is not an end in itself but a means of committing a terrorist attack. With terrorist financing, it is irrelevant whether the funds in question come from legal or illegal sources. In fact, terrorist financing often involves funds that, before being sent, are not related to any illegal activity. Examples have been found in the donation of legitimate funds to charitable organizations, which, sometimes unbeknownst to donors, are in fact fronts of terrorist organizations.
Insurance intermediaries: Entities legally authorized to conduct insurance intermediation, such as insurance brokers, agents and promoters.
Suspicious Operations Reporting Officer: employee at the obliged entity level, responsible for providing due information to GIFiM and taking all other steps, in accordance with the law and the provisions of the respective guidelines.
Insurance premium: Cash benefit, unless otherwise provided by the policyholder to the insurer for the coverage or benefits or reparations guaranteed in a policy, as a consideration for the risk assumed by the same insurer.
Politically Exposed Persons (PPE): Individuals to whom prominent public functions are or have been committed, such as Head of State or Government, senior political staff, senior government, judicial or military positions, senior public enterprise staff and senior civil servants, political parties, as well as close family members and persons with whom they are known to have corporate or commercial relations. For this purpose, the following shall be considered:
a) Senior positions of a political or public nature:
i. Head of State, Head of Government and

members of Government, namely, Ministers, Deputy Ministers and Secretaries of State;
ii. Members or members of parliamentary chambers;
iii. Magistrates of supreme courts, constitutional courts, the Court of Auditors and other high-level judicial bodies whose decisions cannot be appealed except in exceptional circumstances;
iv. Members of the administrative and supervisory bodies of
central banks;
v. Heads of diplomatic missions and consular posts;
saw. High-ranking officers of the Armed Forces;
vii. Members of the management and supervisory bodies of public companies and public limited companies exclusively or mainly public, public institutes, public foundations, public establishments, by whatever means of their designation, including the management bodies of companies in the sectors regional and local businesses;
viii. Members of the executive bodies of International right.
b) Close family members:
i. Spouse or persons with whom they are living in de facto union;
ii. Parents, children and their spouses, or persons with
who are living in de facto union;
c) Persons with recognized and close corporate or commercial relationships:
i. Any natural person who is known to be a joint owner, the holder of a high political or public office of a legal person or with whom he has close business relationships;
ii. Any natural person who owns the share capital or voting rights of a legal person or the assets of a collective interest center without legal personality, who is known as the sole beneficial owner of the high-ranking political or public
Business relationship: agreement between the insurer and the policyholder leading to the completion of transactions during the term of the insurance contract.
Reinsurer: An entity, whether a corporation, headquartered in the Republic of Mozambique or branch, authorized to enter into reinsurance contracts.
Risk: susceptibility to verification of laundering acts
of capital.
Insured: person, natural or legal, in whose interest the contract is entered into or the person (insured person) whose life, health or physical integrity is insured.
Transactions: claims and proposals for an insurance policy, premium payments, claims for benefit changes, beneficiaries, duration, and more.