Thursday, November 17, 2022

SERIES I — Number 222

OFFICIAL GAZETTE

OFFICIAL PUBLICATION OF THE REPUBLIC OF MOZAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.

NOTICE

The information to be published in the Official Gazette of the Republic shall be submitted in a duly certified copy, one for each matter, including, in addition to the indications for the purpose, the following endorsement, signed and authenticated:

For publication in the «Official Gazette».

SUMMARY

Banco de Moçambique:

Notice No. 5/GBM/2022:

Approves the Guidelines on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing.

BANCO DE MOÇAMBIQUE

Notice No. 5/GBM/2022

of November 17

Law No. 11/2022, of July 7, lays down the new framework for Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing in Mozambique.

In light of the need to steer the operations of financial institutions that, as per the Law concerned, are under its scope of supervision, the Banco de Moçambique, in the exercise of the powers conferred thereto by the provisions of Article 54 (*a*) and Article 4 (1) to (4) of the Law concerned, determines as follows:

1. The Guidelines on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing, as attached to this Notice, are hereby approved, and shall constitute an integral part thereof.

2. Failure to comply with the rules provided herein shall constitute a misdemeanor punishable under Law No. 11/2022, of July 7.

3. Notice No. 4/GBM/2015, of June 17, Guidelines on Anti-Money Laundering and Counter-Terrorist Financing, is hereby repealed.

4. This Notice shall come into effect within sixty days, from the date of publication.

5. Any doubts arising from the interpretation and implementation of this Notice are to be submitted to the Regulation and Licensing Department of the Banco de Moçambique.

Maputo, September 2, 2022. - Governor, *Rogerio Lucas Zandamela*.

Guidelines on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing

CHAPTER I

General provisions

ARTICLE 1

Object

These Guidelines lay down anti-money laundering, counter terrorist and counter proliferation of weapons of mass destruction financing procedures and measures.

ARTICLE 2

Scope of Implementation

1. These guidelines shall apply to all financial institutions that, pursuant to paragraphs 1 to 4 of Law No. 11/2022, of July 7, are under the supervision and monitoring of the Banco de Moçambique.

2. Financial institutions other than banks and microbanks are subject to the rules set out herein, to the extent applicable thereto.

CHAPTER II

Risk management policies

ARTICLE 3

Responsibilities of the Board of Directors or equivalent body

1. The Board of Directors or an equivalent body of financial institutions shall document and approve policies on identifying, assessing and managing risk and internal control measures that allow for effectively managing and mitigating identified risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, and submit them to the Banco de Moçambique.

2. For the purpose of the preceding paragraph, the Board of Directors or equivalent body shall favor a risk-based approach.

3. The Board of Directors or equivalent body shall annually approve the institutions' risk assessment policy, determine the level of risk that the institution is willing to accept and propose appropriate risk mitigation measures.

4. As a minimum, the Board of Directors or equivalent body shall annually:

a) formally communicate risk tolerance and risk acceptance strategies to all institution employees; and

b) disclose the recommendations on the implementation of the policy for anti-money laundering, counter-terrorist proliferation of weapons of mass destruction financing.

5. The Board of Directors or an equivalent body shall make sure that the control process and procedures adopted are effective, and add to lowering the risk of the institution being used for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

ARTICLE 4

Risk Management Policy

The risk management policy for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction shall comprise the following:

a) policies and procedures on the duty of identification and verification;

b) policies and procedures on risk assessment, management and monitoring;

c) privacy policies for accounts that are monitored for suspicious transactions;

d) policies and procedures on reporting suspicious transactions and other types of reports;

e) policies and procedures on the safekeeping of documents.

ARTICLE 5

Risk assessment

1. Every year, financial institutions shall carry out a documented risk assessment for all risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, which shall require the approval of the Board of Directors or an equivalent body.

2. In the process of preparing the risk assessment, the institution shall make use of internal information, such as operational and transactional data, as well as external information, such as national and sectoral risk assessment reports.

3. The risk assessment shall be prepared using quantitative and qualitative elements and shall be updated when there is any change in the assumptions used for its preparation that may have a material impact.

4. The risk assessment must be formally approved by the Board of Director or equivalent body, by means of minutes, comprising the following points:

a) products and services provided to customers;

b) specifics of the transactions of the institution, including the nature, complexity, etc.;

c) direct or indirect distribution channels;

d) customer characteristics; and

e) geographic areas where your customers or related transactions are located.

5. The risk assessment shall consider all jurisdictions with which the institution has a business relationship and all possible types of transactions, including:

a) documentary credits;

b) banking correspondents; and

c) transfers.

ARTICLE 6

Implementation of Risk Mitigation Measures

The Board of Directors or equivalent shall ensure the implementation of the mitigation measures approved as part of the risk assessment.

ARTICLE 7

Confidentiality Procedures

1. The procedures of financial institutions on secrecy shall contain provisions on the confidentiality of the existence, content and follow-up of the reporting of suspicious transactions, in order to avoid tipping-off.

2. Tipping-off constitutes a criminal offense, as per Article 206 of Law No. 20/2020, of December 31.

CHAPTER III

Suspicious Transaction Reporting Officer

ARTICLE 8

Appointment

1. The Board of Directors or an equivalent body shall appoint a Suspicious Transaction Reporting Officer (STRO) for the head office, agencies, branches and other forms of institution representation, and guarantee sufficient resources for their activity, namely human, material and technological resources.

2. The STRO shall be elected from the institution's management level employees, and shall, as a minimum, boast a high-level of responsibility and independence.

3. The level of resources referred to in paragraph 1 of this Article shall reflect the dimension, complexity, number of customers and products provided by the institution.

ARTICLE 9

Responsibilities of the Suspicious Transaction Reporting Officer

1. The STRO shall support and steer the risk management for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction at the financial institution.

2. Without prejudice to the provisions of other applicable legislation, the STRO's responsibilities are as follows:

a) regularly review the adequacy of the system of controls on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing, including:

i. Inspecting the implementation of policies and procedures on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing;

ii. ensuring an appropriate monitoring process; and

iii. actively participating in the choice of software to monitor customers and their transactions;

b) ensure that all relevant information is transmitted to employees, monitoring compliance with the policies on training and capacity building approved by the institution and ensuring that its content is appropriate, updated and aligned with good practices and trends in the phenomenon of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

ARTICLE 10

Confidentiality

1. STROs shall observe confidentiality against all individual alerts, transactions and suspicious transactions they should handle during their time of office.

2. The exchange of information within the institution shall only be made with persons of the organization subject to the same obligation of confidentiality in cases of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction on a need-to-know basis, as set out in the financial institution procedures.

ARTICLE 11

Centralized Coordination

1. Financial institutions shall appoint a coordinating STRO, tasked with coordinating and centralizing information received from other STROs, and analyze suspicious transactions identified.

2. The coordinating STRO is particularly responsible for:

a) ensure the submission of suspicious transaction reports to the Mozambique Financial Information Office (GIFiM), with all relevant information about the transaction and the customer;

b) ensure the prompt submission of all additional information requested by the competent authorities with regard to suspected cases of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction; and

c) ensure centralized coordination with several stakeholders, including internal auditors, external auditors, the Banco de Moçambique, the GIFiM and judicial and administrative authorities.

ARTICLE 12

Replacement

1. If there is need to replace an STRO, due to absence or otherwise, the financial institution shall ensure that the replacement meets the requirements.

2. In order to avoid conflicts of interest, under no circumstances shall a STRO be replaced by a member from internal auditing.

ARTICLE 13

Conflicts of Interest

The Board of Directors or an equivalent body shall adopt provisions for the prevention of conflicts of interest for STROs, including the prohibition of establishing incentives that may constitute hindrances for the timely identification and reporting of suspicious transactions to the competent authorities.

CHAPTER IV

Internal Audit

ARTICLE 14

Internal Auditing Responsibilities

Internal audit shall be responsible for carrying out an independent assessment and for the effectiveness and efficiency of the system for anti-money laundering, counter-terrorist and financing of proliferation of weapons of mass destruction. That said, it must:

a) verify the adequacy of policies;

b) adopt procedures and support systems to detect potential suspicious transactions of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction;

c) assess whether each line of defense adequately performs its assigned tasks and functions;

d) review the system's operation, so as to ensure proper performance.

ARTICLE 15

Independence

Internal auditing shall always be independent, and report directly to the Board of Directors or equivalent body.

ARTICLE 16

Internal auditing program and report

1. The internal audit program should be aligned with the risk assessment carried out by the financial institution.

2. The internal auditing report shall be presented, in good time, to the Board of Directors or equivalent body and to the auditing committee, if any.

ARTICLE 17

Scope and methodology

The Board of Directors or equivalent body shall ensure that the scope and methodology of internal auditing are suitable to the risk profile of the financial institution, and that the frequency of the audits is risk-based.

ARTICLE 18

Findings

Any adverse findings from the internal audit shall be duly presented to the Board of Directors or equivalent body, in accordance with the formal corporate governance structure.

ARTICLE 19

Duties of Internal Auditing

1. Internal audit shall ensure compliance with procedures for Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing,

at all agencies and branches of the financial institution.

2. The duty referred to in the preceding paragraph shall cover third parties and agents acting on behalf of the financial institution to ensure its compliance with the policies and procedures of the financial institution.

3. Internal auditing shall particularly review due diligence and Know Your Customer processes for customers, products, services or distribution channels identified as high-risk.

4. Internal auditing shall check for the diligent handling of alerts on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, and if said generated alerts are promptly terminated with an appropriate risk assessment.

ARTICLE 20

Frequency

Internal audits shall be carried out on the whole or part of the financial institution's system on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing at least annually.

CHAPTER V

Outsourcing and Organization of Groups

ARTICLE 21

Outsourcing

A financial institution that outsources operational activities, comprising or associated with duties of Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing to service providers, shall verify that its procedures are effectively implemented by the service provider, especially if these are located abroad.

ARTICLE 22

Group Relationship

1. If the financial institution belongs to a group or is the parent company of a financial group, internal procedures shall allow the sharing of information within the group for the purposes of organizing and monitoring anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction, including the forwarding of information to the group's parent company.

2. The procedures for sharing information shall be in accordance with the relevant legislation.

ARTICLE 23

Principle of Equivalence

If the financial institution is the parent company of a financial group, the STRO responsible for implementing the risk management policy for money laundering, counter-terrorist and proliferation of weapons of mass destruction financing of the group must check if the measures applied in entities abroad are, at least, equivalent to those in effect in Mozambique, and if the branches in other States fulfill provisions similar to those of Mozambique.

ARTICLE 24

Communications

If the financial institution is the parent company of a financial group, the STRO responsible for implementing the group's system must be informed of reports of suspicious transactions made to a Financial Reporting Unit by any group entity.

ARTICLE 25

Branches

If the financial institution has branches, the STRO responsible for implementing the group's system shall verify if the local legislation applicable does not prevent quick access to transaction documents or details.

CHAPTER VI

Duty of identification and verification

SECTION I

Customer policies and classification

ARTICLE 26

Know Your Customer

1. Financial institutions shall adopt policies on the identification and verification of their customers, irrespective of the amount of individual transactions.

2. The "Know Your Customer" policy of financial institutions shall comprise the following items:

a) customer acceptance policy;
b) customer identification and verification procedures;
c) operations monitoring; and
d) risk management.

ARTICLE 27

Customer acceptance policy

Financial institutions shall draw up a clear policy on customer acceptance, including measures applicable for each customer category.

ARTICLE 28

Customer Acceptance Policy Content

1. The customer acceptance policy shall consider risks associated with the customer, country or geographic region, and risks associated with the product delivery channel, service or operation, as examples set out in Annex I to this Notice.

2. In essence, the customer acceptance policy shall comprise, but not be limited to, the following:

a) prohibition of opening anonymous or fictitious accounts;
b) prohibition of opening numbered accounts;
c) categorizing the customer regarding the risk assessment carried out;
d) necessary documentation, additional information to be required and applicable measures for each category of customer, based on the risk assessment carried out;

e) enhanced due diligence measures for the acceptance of high-risk customers, as exemplified in Annex II;

f) prohibition of opening or closing an account when the financial institution is unable to apply due diligence measures;

g) the circumstances in which the customer is allowed to act on behalf of another, an individual or a legal entity, must be clear and in accordance with the legislation in force; and

h) types of background checks necessary, prior to opening the account, in order to verify if the customer does not have a criminal record, Is on terrorist or terrorist organization lists.

ARTICLE 29

Risk Classification

1. Financial institutions shall have a clear and active risk rating policy for their customers.
2. Customer risk rating needs to be updated, at least once a year.
3. The frequency of risk rating should be increased for high-risk customer cases.

ARTICLE 30

Trigger Management System

Financial institutions shall have an appropriate trigger management system that allows to carry out the necessary evaluation of the customer acceptance process in light of any events that the customer may undergo, and that may imply a review of the respective risk classification.

SECTION II

Customer identification and verification procedures

ARTICLE 31

Duty of Identification

Financial institutions shall identity their customer as per the terms and situations provided for in Law No. 11/2022, of July 7, and whenever they lack sufficient and current information about the customer.

ARTICLE 32

Duty of Verification

1. Financial institutions shall identity and verify the identity and current address of their customers and learn the nature of the customer's businesses, income sources, financial standing and the type of business relationship they desire with the institution.

2. Financial institutions shall ensure, as far as possible, that the customer is an upstanding person, and verify their identity, in accordance with the provisions of this Chapter.

ARTICLE 33

Intermediaries

1. If the funds to be deposited or transferred are being provided by a third party, the institution shall identify and verify that person.

2. If the institution is unable to determine whether the applicant in the business is acting on its own or on the behalf of a third party, it should consider submitting a suspicious transaction report to GIFiM, even if the account is not opened or the transaction is not processed.

ARTICLE 34

Surveillance Measures

Financial institutions shall require customers to provide, in writing, the identity and information of natural persons who are the actual beneficiaries of the business relationship or transaction, as part of monitoring measures to identify and verify the identity of the individuals.

ARTICLE 35

Confirmation of Identity

1. Financial institutions shall obtain all information necessary to confirm the identity of the customer and verify the information provided by the customer.

2. For the purpose of the provisions of the preceding paragraph, financial institutions may use available national and international public information, cross-check information with other evidence, namely the invoices for water supply, electricity and telephone, telephone directories, credit registration centers, criminal records, and safe keep this information in their files.

ARTICLE 36

Identity of the Actual Beneficiary

If the customer is not the beneficiary of the business relationship, the financial institution shall take reasonable steps to verify the identity of the actual beneficiary, using relevant information or data obtained from a source it deems appropriate to support it.

ARTICLE 37

Closure of accounts

1. When a customer closes one account and requests the opening of another at the same financial institution, the duty of identification and verification is not waived, and in this case, the details on the customer's file must be reconfirmed.

2. The details of the accounts and the steps taken pursuant to the preceding paragraph to verify the identity and the records made shall be transferred to the records of the new account.

ARTICLE 38

Change of identification details

1. Any subsequent change in the customer's name, address, or information about their employment status of which the institution is aware shall be recorded and duly substantiated by documentary evidence as part of the due diligence process.

2. Customer and beneficial owner information
shall be kept on file.

ARTICLE 39

Account balance transfer

1. If a customer transfers the balance of an account they held with one financial institution to another, the receiving institution shall consider the possibility that the previous account manager has suspicions about the customer's activities.

2. If the receiving institution has any reason to suspect that the customer has been rejected by another financial institution, it must apply enhanced due diligence procedures before accepting the customer.

ARTICLE 40

Confirmation of identity by interview

1. For individual accounts, financial institutions shall ensure that proof of identity is obtained during the course of an interview with the customer in order to ascertain whether the customer is indeed the person they claim to be and to ascertain the similarity between the person and the photograph on the identity document.

2. In the case of joint accounts, financial institutions should verify the names and addresses of all account holders.

3. The verification procedures necessary to establish the identity of the customer must be the same, regardless of the type of account, i.e., current account, deposit account, among others.

ARTICLE 41

Employee identification

The name of the employee of the institution that led the account opening process and the senior manager who authorized must be included in the customer's file.

ARTICLE 42

Business and asset control

Financial institutions shall identify and verify persons or entities that hold control over the business and assets of customers.

ARTICLE 43

Third-party introducers

When using one or more agents or third-party introducers in order to form business relationships with customers, financial institutions are the only entities liable for completing due diligence against the customers introduced.

ARTICLE 44

Duty to refuse

1. Whenever a financial institution is unable to obtain all the necessary due diligence information, it shall not open the account, enter into the business relationship nor carry out the transaction.

2. In the cases provided for in the preceding paragraph, the financial institution shall consider reporting the suspicious information to the GiFiM.

SECTION III

Opening accounts

SUBSECTION I

Individual customers

ARTICLE 45

Account opening by individual customers

In cases where the customer is a natural person, the identification must be supported by the presentation of one of the official documents referred to in Article 5 (2) of Decree No. 66/2014, of October 29, considering the risk category thereof.

ARTICLE 46

In-person account opening by individual customers

1. The identification of an individual customer shall comprise:

a) name;
b) date of birth;
c) physical address;
d) nature of the business;
e) source of income;
f) level knowledge about standard financial transactions; and
g) any representation relationship.

2. The name of individual customers must be verified by a valid document, during an interview with said customer.

ARTICLE 47

Address confirmation

For the purposes of Article 6 (1) (a) of Decree No. 66/2014, of October 29, the following shall be considered suitable for address confirmation:

a) invoices issued for electricity, water, telephone and internet supply services ;
b) telephone directory information;
c) recent credit or debit card statement from another financial institution;
d) recent bank reference; and
e) any other document that individually or cumulatively proves the address of the applicant for the business, namely the declaration of the neighborhood office and the employer.

ARTICLE 48

Individual customer account opening forms

1. The account opening form for an individual customer must, at a minimum, contain the following information:

a) name;
b) current permanent address;
c) mailing address;
d) telephone and fax number;
e) e-mail address, if any;
f) date and place of birth;
g) nationality;

h) occupation and name of employer (if self-employed, the nature of business and the confirmation concerned);
i) Individual Taxpayer Identification Number (NUIT);
j) Economic Activity Classification Code (CAE), for businesses;
k) signature(s); and
l) authorization for the financial institution to probe and obtain references about the customer.

2. A legible copy of the identification document used, and all documentation related to the verification of the customer's identity, must be attached to the duly completed form.

ARTICLE 49

Identity verification in cases of non-in-person account opening

Prior to entering into a business relationship with a non-in-person customer,
the financial institutions must:

a) adopt customer identification procedures applicable to in-person customers, and promptly set up the interview; and
b) take enhanced due diligence measures in order to mitigate the risk associated with the non-in-person customer.

ARTICLE 50

Account opening by non-resident individual customers

1. Non-resident individual customers applying to open an account abroad must complete an application form, with, at least, the following information:

a) name;
b) permanent address;
c) current address;
d) telephone number and fax number;
e) e-mail address, if any;
f) date and place of birth;
g) nationality;
h) occupation and name of employer(if self-employed, the nature of the business)
i) number, date of issue and date of validity of the passport;
j) Signature(s);
k) reference letter from the customer's banking institution at the
current country of residence; and
l) authorization so the financial institution can carry out a background check on references of potential customers.

2. The application form duly completed must be supported by a copy of a valid passport and address information, confirmed by an original or certified copy of an invoice issued by third-party service providers, namely electricity, water, telephone and internet service providers, etc.

3. Financial institutions may also request, as additional measures related to address verification, consultation of the telephone directory or inquiries with financial institutions or other entities in the customer's country of residence or consultations with national or international sources that the requested institution considers appropriate.

SUBSECTION II

Legal persons

ARTICLE 51

Account opening by legal persons

1. During the legal person account opening process, financial institutions shall verify:

a) the identification of the shareholders controlling the company's businesses and assets;
b) the identification of their senior managers;
c) the identification of all holders of qualified stakes;
d) the identification of all holders of unregistered shares valued at 10% or more;
e) identification of persons authorized to represent the company;
f) Individual Taxpayer Identification Number (NUIT);
g) The Economic Activity Classification Code (CAE); and
h) evidence of the legal existence of the company.

2. In the identification and verification process, the items indicated Article 5 (4) of Decree No. 66/2014, of October 29, must be presented.

3. In the case of agricultural associations, the identification details set out in Article 5 (4) *(a)* of Decree referred to in the preceding paragraph are replaceable by a certificate of recognition issued by the district administrator or head of the administrative post of its headquarters, as provided for in Decree-Law No. 2/2006, May 3.

ARTICLE 52

Visits to legal persons

In high-risk situations, verification and consultations shall be carried out by visiting said legal persons, in order to ascertain their existence, as well as the absence of any dissolution or liquidation procedure, and confirm the economic purpose, as provided by the permit or with the supervisory authority.

ARTICLE 53

Monitoring procedures

1. The "Know Your Customer" due diligence on legal person accounts must be an ongoing process, just as the individual customer accounts.

2. If there are changes in the structure of the legal person or if suspicions are aroused by a change in the business nature or payment or receipts profile in the legal person's account, other verifications must be carried out in order to ascertain the reason for such changes.

ARTICLE 54

Account opening by non-resident legal persons

The identification and verification process referred to in Articles 51 to 53 shall also be applicable, with the necessary adaptations, to non-resident legal persons intent on opening an account from abroad.

ARTICLE 55

Tax information

1. Financial institutions must, at the time of opening a bank deposit account, obtain information on the Individual Taxpayer Identification Number (NUIT) from each of the respective holders.

2. The NUIT can be confirmed by presenting the original or notarized copy of a document with that number, or by obtaining and verifying said information with management authorities.

ARTICLE 56

Consortia and incorporated businesses

1. For companies formed as consortia or undertakings without legal personality, the identification and verification of persons that hold control, of shareholders with qualified stakes and their representatives shall also comply with the necessary adaptations to the provisions set out in Articles 45 to 50.

2. Financial institutions shall carry out verifications so as to confirm the true nature of the business nature and if said business is underpinned by a legitimate purpose.

ARTICLE 57

Clubs and charities

Before opening accounts for clubs or charities, financial institutions should:

a) confirm the legitimate purpose of the organization;
b) request a notarized copy of the formation of the club or charity; and
c) if in doubt, visit their premises to learn the true nature of their business.

ARTICLE 58

Identification and verification of persons controlling the club or charity

1. The identification and verification of persons holding control over the club or charity shall be determined based on the necessary procedures concerning individual customers.

2. Changes within the club or charity shall require further identification and verification due diligence.

ARTICLE 59

Foundations and associations

The identification and verification of a foundation or association includes, among others, the following items:

a) name;
b) certificate of formation;
c) date and country of formation, in the case of foreign entities;
d) business address; and
e) main place of business and operations, should it differ from the business address.

ARTICLE 60

Foundation or association verification procedures

1. Due diligence for the verification of the foundation or association shall be carried out by submitting the following information:

a) certificate of formation issued by the competent authority;
b) financial statements for the past two years; and
c) other additional information deemed relevant.

2. The identification of the persons that head the foundation or association cover board members or the equivalent body, especially of those with authority to carry out business or provide orders on the using or transferring funds or goods, the founder, the executor, the protector, the payee and the administrator.

3. If charitable, the found or association shall be bound to rules concerning the identification of clubs and charities.

SECTION IV

Foreign persons and financial institutions

ARTICLE 61

Correspondent banks

1. In business relations with correspondent banks, financial institutions shall:

a) gather enough information about their correspondents in order to understand the nature of their business;
b) ascertain, from publicly available information, the reputation and regulatory and supervisory quality of the institution, including if it had been the subject of any investigation or action related to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction;
c) evaluate control systems on anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction and check if they are adequate and effective;
d) obtain authorization from the competent senior management body of the institution, prior to entering into new relationships of correspondence; and
e) document the responsibilities of each institution, inter alia, regarding anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction.

2. For the purposes of Paragraph 1 *a*) of this Article, the following factors shall be considered:

a) information on the correspondent's management;
b) main business activities;
c) location;
d) Regime of Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing; and
e) identification of third parties using the corresponding services.

ARTICLE 62

Payable-through accounts

In the case of payable-through accounts, financial institutions shall ensure that the customer bank has applied ongoing due diligence measures against the customer with direct access to the correspondent bank's accounts and that said bank is able to provide the relevant data on the identification of their customers, when the correspondent bank requests it.

ARTICLE 63

Shell banks

Financial institutions shall in particular refuse to enter into or maintain a relationship with the correspondent if it does not have a physical address and is not part of a regulated financial group (shell banks).

ARTICLE 64

Non-cooperative countries

1. Financial institutions shall apply enhanced due diligence measures when a business relationship or transactions with legal persons and financial institutions of countries deemed non-cooperative by the Financial Action Task Force (FATF), and the Banco de Moçambique is responsible for disclosing said list by Circular.

2. In light of the risk-based approach, financial institutions shall apply enhanced surveillance measures for business relationships or transactions with legal persons and financial institutions of countries identified as high-risk in their annual risk assessment or by other sources, such as the National Risk Assessment, sectoral risk assessments, etc.

SECTION V

Politically Exposed Persons

ARTICLE 65

Duties of financial institutions

Without prejudice to the provisions provided by other legislation,
financial institutions shall:

a) adopt appropriate risk management systems to determine whether a potential customer, an existing customer or the actual beneficiary is a Politically Exposed Person (PEP);

b) develop a clear policy, proper internal control procedures and remain vigilant as to business relationships with PEPs, people and companies clearly related or associated with them or other high-risk customers;

c) take reasonable steps to determine the sources of wealth and resources of the customer and beneficiaries identified as PEP;

d) obtain approval from senior management prior to entering into a business relationship with a PEP;

e) draw up a list of PEP with a bad reputation and update it regularly, whenever necessary, based on reliable sources of information, such as the media/news, etc.;

f) publish information on the enhanced due diligence measures applicable to the business on their official website; and

g) identify PEPs in the country concerned and ascertain if the customer has family or business ties with said persons, whenever they maintain business relationships with customers from countries whose public and credible information suggest that they are vulnerable to corruption.

ARTICLE 66

Ongoing monitoring

1. Financial institutions shall undertake ongoing monitoring, considering that customers may form ties with PEPs following the establishment of the business relationship.

2. Given that PEP may initially be identified as such, and that current customers may at a later time become PEPs, the institution shall regularly revise their customers at least every twelve months.

SECTION VI

Wire transfers

ARTICLE 67

International wire transfers

1. In order to ensure that the wire transfer system is not used for unlawful purposes, without prejudice to other applicable legislation, financial institutions shall ensure that correct payer information and required payee information is available.

2. Financial institutions shall include in all transfers of funds, related messages.

3. The messages referred to in the preceding paragraph shall remain in the payment transfer chain until their final destination.

4. The information supporting all wire transfers shall include:

a) name of payer;

b) payer's account number, if the account was used for processing the transaction;

c) payer's address;

d) national identification document number or customer identification number;

e) date and place of birth;

f) name of payee;

g) payee account number, if that account is used for operation processing;

h) beneficiary banking institution; and

i) transaction value.

5. In cases of absence of an account, the single reference number of the operation that allows for screening must be included.

ARTICLE 68

Transfers processed by an intermediary

1. Whenever transfers of funds are processed by an intermediary and in the amounts defined by Article 24 (3) of Decree No. 66/2014, of October 29,

the financial institution acting as an intermediary in the wire transfer chain shall ensure that all information on the payer and the payee, accompanying the transfer is retained and, where possible, included in the message generated.

2. In the case that technical limitations prevent that the necessary information on the payer or payee to accompany an international wire transfer be conveyed with the corresponding domestic wire transfer, the receiving intermediary financial institution shall be liable for safekeeping records of all information received from the payer financial institution or any other intermediary financial institutions for at least ten years.

ARTICLE 69

Control measures

1. The intermediary financial institution shall take reasonable control measures to identify international wire transfers where necessary information about the payer or payee is missing.

2. The measures referred to in the preceding paragraph may include follow-up or real-time monitoring where possible.

ARTICLE 70

Risk-based policies and procedures

The intermediary financial institutions shall have effective risk-based policies and procedures in place to determine:

a) when it must carry out, reject or suspend a wire transfer, when necessary information about the payer or payee is missing;

b) appropriate follow-up activities.

ARTICLE 71

Reporting to the Mozambique Financial Information Office

The absence of complete information on the payer may provide for suspicion and consequently the intermediary financial institution shall consider the possibility of reporting to the GIFiM.

ARTICLE 72

Restriction or termination of the business relationship

The payee financial institution shall consider restricting or even terminating the business relationship with financial institutions that do not meet the requirements referred to in the previous articles.

ARTICLE 73

Domestic wire transfers

1. Domestic wire transfers shall include information on the payer, as provided in international wire transfers, unless if the information can be provided by the payee financial institution to the competent authorities, namely the GIFiM and judicial authorities.

2. In the cases referred to in the preceding paragraph, the payer financial institution only needs to include the account number or the single transaction reference number, provided that this number allows for identifying that the transaction is associated with the payer or payee.

3. The information referred in the preceding paragraphs shall be made available by the payer financial institution within three working days, following the receipt of the request by the payee institution or the authorities also referred to in Paragraph 1.

SECTION VII

Mobile Money

ARTICLE 74

Identification and verification procedures

1. The procedures for identifying users of mobile money shall include the verification of the customer's identity, regardless of the amount converted to mobile money from banknotes and currency in circulation (physical currency).

2. Procedures shall also include the implementation of enhanced surveillance measures during the repayment or withdrawal of mobile money over a certain limit set out by financial institutions.

ARTICLE 75

Collection and storage of information and data

1. Procedures for converting mobile money shall comprise the collection and storage of technical information and data on the activation, top up and use of mobile money by means of physical support for screening purposes.

2. The financial institution shall retain the information for a minimum of ten years.

SECTION VIII

Account and transaction monitoring

ARTICLE 76

Ongoing monitoring

Ongoing monitoring as an essential aspect for managing risk of money laundering, financing of terrorism and the proliferation of weapons of mass destruction , must include the screening of transactions made during the relationship with the customer in order to ensure that they are consistent with the financial institution's knowledge on the customers, namely business and risk profile.

ARTICLE 77

Transaction reconstruction

1. In order to enable transaction reconstruction, financial institutions shall ensure that the documents presented or information collected in light of due diligence measures are kept up to date and relevant.

2. Relevance is ascertained by reviews of existing records and analysis of transactions, especially for categories of customers or business relationships of the highest risk.

ARTICLE 78

Risk assessment

1. Monitoring shall fall in line with risk assessment and must have systems in place to detect complex, uncommon or suspicious transactions standards for all accounts.

2. In light of risk assessment, financial institutions shall ponder that some types of transactions and activities may alert them to the possibility of acts of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

3. Examples of suspicious transactions and activities can be further explored by consulting the typologies on money laundering, terrorist financing or financing of proliferation of weapons of mass destruction published by the Financial Action Task Force (FATF) at *http://www.fatf-gafi.org* and Annex III to this Notice.

ARTICLE 79

High-risk accounts

Financial institutions shall escalate high-risk accounts' monitoring by setting up key-indicators for said accounts, based on the known customer's information, for example:

a) country of origin;
b) sources of resources;
c) the type of transactions involved; and
d) other risk factors.

ARTICLE 80

Management information systems

Financial institutions shall have proper management information systems in place in order to provided managers and STROs with up-to-date information to identify, analyze and monitor accounts.

CHAPTER VII

Financial innovations

ARTICLE 81

Prevention policies and measures

1. Financial institutions shall adopt the necessary policies or measures to prevent the misuse of technological developments in schemes for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

2. Financial institutions shall identify, assess and understand the money laundering, terrorist financing and weapons of mass destruction proliferation financing risks associated with all new or pre-existing products, services and distribution channels and the use of new technologies.

ARTICLE 82

Risk assessment

Financial institutions shall carry out the risk assessment prior to the introduction of new products, services, delivery channels and technologies and shall implement the necessary measures to effectively manage the concerning money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks.

CHAPTER VIII

Safekeeping of documents

ARTICLE 83

Identification records

All documentation required by financial institutions, pursuant to this Notice and other applicable legislation, to verify the identity of customers and actual beneficiaries shall undergo safekeeping for a period of not less than ten years after the closure of the account or termination of the business relationship
with the customer concerned.

ARTICLE 84

Outsourcing

Should the financial institution decide to hire the services of a third party to undertake the verification of identification procedures or confirm the identity of customers, the safekeeping of documents shall comply with the provisions set out in the previous paragraph.

ARTICLE 85

Transaction records

Transaction records, regardless of the manner of use, shall be kept for a period of not less than ten years after the completion of the transactions concerned in order to assist in the investigation of cases of suspected money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction and shall include
the following:

a) Turnover through the account;
b) origin of funds, including all customer details;
c) how funds were credited or debited from the account;
d) identity of the person carrying out the transaction and the identity of the actual beneficiary;
e) counterparty details;
f) destination of funds;
g) form of instruction;
h) date of transaction;
i) type and identification number of any account involved in the transaction; and
j) any other information that allows for reconstructing the transaction.

ARTICLE 86

Document safekeeping term

The internal report on anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction, the reports on suspicious transactions, cash transactions, electronic fund transactions and cheques sent to the GIFiM shall be kept for not less than ten years following the date of drawing up.

ARTICLE 87

Safekeeping of findings

Without prejudice to the provisions of the preceding article, all conclusions concerning complex, uncommon suspicious and other transactions that not falling in line with said characteristics are part of the transactions to be reported to he GIFiM shall be kept for a period not less than ten years, from the date of the finding concerned.

ARTICLE 88

Safekeeping of information on ongoing investigations

1. Records concerning ongoing investigations shall be kept until the competent authorities confirm that the case has been closed.

2. The confirmation of cases closed by the authorities shall be filed and include the documentation stating the reason for closure.

3. Policies and procedures shall outline the criteria and protocol used to close cases and indicate the records that no longer require safekeeping.

ARTICLE 89

Safekeeping of transactions by electronic means

Electronic payment records and the relating messages shall be handled as provided for in the preceding articles.

CHAPTER IX

Recognizing and Reporting Suspicious Transactions

ARTICLE 90

Recognizing suspicious transactions

1. Employees of financial institutions shall undergo sufficient training and orientation in order to recognize suspicious transactions, as provided for in Chapter X.

2. For example, the points to consider in order to ascertain if a transaction is suspicious may be the following:

a) The volume, quantity or frequency of transactions consistent with the customer's regular or previous business, or their pattern and purpose:

b) the transaction is reasonable or understandable given the customer's businesses or personal activities;

c) the transaction amount compatible with the professional occupation and financial standing declared by the customer;

d) the customer's activity pattern changed materially against the customer's business history or profile;

e) is the degree of complexity and risk of the transaction compatible with the technical qualification of the customer?

f) the transaction is international, and there is a clear reason for the customer to do business with the country concerned; and

g) the transaction makes economic and legal sense, or seems to pursue to hide or obscure another separate transaction.

ARTICLE 91

Updating internal procedures

In the process of updating internal procedures, the financial institution shall always consider the facts and circumstances that gave rise to suspicious transaction reports.

ARTICLE 92

Types of high-risk transactions

Financial institutions shall implement tailored screening and investigation procedures to detect the types of transactions with a high risk of money laundering, terrorist financing and financing and financing of proliferation of weapons of mass destruction provided by Annex IV.

ARTICLE 93

Reporting suspicious transactions

All financial institutions must ensure that:

a) employees at their jobs know whom to report suspicious transactions to;

b) the reporting chain is clear, so that suspicions are directly and immediately informed to the STRO;

c) procedures provide that employees who report risks or problems in suspicious operations are fully protected, exempt from liability and immune from any repercussions; and

d) reconstruction of the transaction is possible.

ARTICLE 94

Reporting suspicious transactions

Financial institutions shall be registered in the GIFiM computer system, with a registration number and a form access password to be assigned to the STRO.

ARTICLE 95

Contents of the suspicious transaction report

Every suspicious transaction report sent to GIFiM, using the form, manual or electronic, shall bear the following information:

a) financial institution sending the report;

b) bank account number involved in the transaction;

c) account holder;

d) transaction executor;

e) monetary value of the transaction;

f) summary description of the nature of the transaction and all circumstances giving rise to suspicion;

g) business relationship between the suspect and the financial institution;

h) when the suspect is an internal customer of the financial institution (employee), reference to this quality;

i) any voluntary statement of the origin, source or destination of resources;

j) impact of suspicious activity on the credibility of the reporting institution or person; and

k) name and signature of the suspicious transaction reporting officer.

ARTICLE 96

Responsibilities of the Suspicious Transaction Reporting Officer

1. The STRO shall ascertain if the information or any other matters comprised in the transaction report received provided for reasonable suspicions that a customer may be engaged in money laundering, terrorist financing and proliferation of weapons of mass destruction.

2. In the assessment, the STRO must consider all important information available on the natural or legal persons to whom the initial report refers to.

3. The aforementioned in the preceding paragraph may include the need to review other transaction patterns and volumes, based on the following information:

a) account or accounts in the same name;
b) duration of the business relationship; and
c) identification records made.

4. If, after completing the review, they determine the existence of suspicious facts, the STRO shall immediately report them to GIFiM.

5. In the reporting of suspicious transactions and performance of their duties, the STRO shall act honestly and rationally and make their judgement based on good faith.

ARTICLE 97

Internal reporting procedure

1. In order to ensure speed and secrecy, the channel for reporting suspicious transactions should be as short as possible, with the least number of players between the employee that detects the suspicion and the STRO.

2. The employee who detects the suspicion may first discuss it with the STRO, and then draw up the initial report and send it. The latter must acknowledge receipt.

3. The report shall include full details of the customer, namely profile, account statements, if necessary, and the full report, as thorough as possible, of the reasons that gave rise to the suspicious.

4. All suspicious transactions reported to the STRO shall be documented.

ARTICLE 98

Investigations

1. All internal investigations made regarding the report, along with the grounds for submission or not to the GIFiM shall be documented.

2. The information referred to in the preceding paragraph may be necessary to supplement the initial report or as evidence of good practice if, at some point in the future, there is an investigation into a case that the STRO decided not to report, and the suspicions are later confirmed.

ARTICLE 99

Format

The standard format for reporting suspicious transactions is drawn up and laid down by the GIFiM, and all financial institutions shall comply with the body's determinations.

CHAPTER X

Screening and Training of Employees and Agents

SECTION I

Screening

ARTICLE 100

Employee screening

1. Financial institutions shall adopt verification procedures in their recruitment policy, in order to ensure a high employee standard.

2. When recruiting, financial institutions shall seek out appropriate references.

ARTICLE 101

Recruitment of agents

Should financial institutions hire agents or distributors for some of their products and services, they should be submitted to screening procedures to assess if they are fit and proper.

SECTION II

Employee training

ARTICLE 102

Ongoing training program

Financial institutions shall implement an ongoing training program for employees on risk management programs and practices.

ARTICLE 103

Requirements for the various employee categories

1. All employees shall receive information on anti-money laundering, counter-terrorist financing and financing of proliferation of weapon of mass destruction in the face of the current legal and regulatory framework of Mozambique, international regulations on the matter and trends and developments relating to the practices concerned.

2. All employees shall also receive information on risk assessment and management.

3. Employees responsible for opening accounts and accepting new customers shall be training on identifying and verifying the identity of customers.

4. Employees shall also be knowledgeable on the recognition and handling of suspicious transactions, as well as with the procedures for reporting suspicious transactions internally.

ARTICLE 104

Training of board members

1. Members of the Board and equivalent bodies and other managers of financial institutions shall receive training on all aspects of the proceedings of anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing.

2. Among other contents, the training of board members, equivalent bodies and other managers of financial institutions shall comprise:

a) risk management policies;
b) penalties arising from the Law in cases of absence of reporting;
c) exclusion of liability in cases of reporting;
d) internal communications procedures;
e) Identity verification requirements;
f) record keeping;
g) allocation of resources for prevention; and
h) consultation of Designated Lists.

ARTICLE 105

Training the Suspicious Transaction Reporting Officer

In addition to general training on anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing, the STRO shall undergo training comprising:

a) all matters of financial intelligence;
b) internal policies applicable in their institutions;
c) recognition of suspicious transactions;
d) initial and ongoing instruction on the validation and reporting of suspicious transactions;
e) framework for the return of suspicious information forwarded; and
f) new types and trends of the legal type of crime.

ARTICLE 106

Newly hired employees

1. Newly hired employees shall, at the earliest opportunity, receive general training on anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing and the internal procedures adopted for the reporting of suspicious transactions.

2. The employees referred to in the preceding paragraph shall also have access to all legislation and to the policies and procedures of the institution on anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing.

ARTICLE 107

Front-office

1. Front-office employees shall undergo training in order to learn the true identity of the customer and obtain sufficient information on the type of business expected by the customer so that they are alert to any change in the behavior of their transactions or circumstances that may constitute criminal conduct.

2. Front-office employees shall also undergo training on the recognition and handling of suspicious transactions and procedures to be adopted when a transaction is deemed suspicious.

ARTICLE 108

Wire transfers

Employees carrying out wire transfers shall undergo training on risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction concerning the business and on the preventive measures applicable thereto.

ARTICLE 109

Training of agents and distributors

1. Agents and distributors shall undergo a training and regularly receive information on anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing tailored to their duties.

2. All agents, distributors and other persons acting on behalf and in the name of the financial institution in contact with customers shall be screened, monitored, informed and trained, at least annually, for specific risk factors of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, including operational procedures for the activities relating to the duties.

ARTICLE 110

Refresher course

Every year, financial institutions shall ensure training so as to keep employees and customers aware of their responsibilities.

ARTICLE 111

Records

Financial institutions shall keep records of all training provided to their employees and agents, including contents, beneficiaries and trainer entity.

ARTICLE 112

Internal audit

The internal audit shall test the effectiveness of the annual training on anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing of all personnel concerned in the financial institution, including members of the board or equivalent body.

CHAPTER XI

Risk-Based Supervision

ARTICLE 113

Communications

1. In order to carry out risk-based supervision of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, every semester financial institutions shall report to the Banco de Moçambique, up to the thirtieth of the month following the period concerned, information concerning customer accounts and transactions involving risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, as well as changes to the monitoring and control of said risks.

2. The data and information referred to in the preceding paragraph shall be report with reference to December 31 and June 30 every year and submitted in the Excel format as provided by Annex V.

ARTICLE 114

Designated Lists

The STRO shall consult, on a permanent basis, the Designated Penalties Sanctions laid down by the United National Security Council Resolutions 1267, of 1999 and 1989, and 2011 and request the competent authority to freeze without delay the accounts on that list or terminate any business relationship with said account holders.

CHAPTER XII

Specific Provisions Applicable to Money Remitters and Mobile Money Networks

SECTION I

Initial provisions

ARTICLE 115

Scope

Without prejudice to the provisions of the preceding chapters, this chapter lays down provisions especially applicable to money remitters and mobile money networks and their business, regardless of the manner of remittance used, making for additional due diligence measures.

ARTICLE 116

Appointment of representatives in Mozambique

Money remitters operating in Mozambique from a foreign jurisdiction shall appoint a representative in Mozambique responsible, inter alia, for responding to requests from supervisory authorities and authorities responsible for anti-money laundering, counter-terrorist and weapons of mass destruction proliferation financing.

ARTICLE 117

Risk mapping and monitoring system

1. Money remitters shall:
   a) lay down a specific risk mapping for their transactions in, to and from Mozambique and apply tailored methods to identify potentially suspicious transactions; and
   b) implement consolidated monitoring, including all transactions in, from and to Mozambique, regardless of the network of bank branches, agents or jurisdictions through with said transactions pass.
2. The characteristics of the risk mapping and monitoring system shall be reported annually to the Banco de Moçambique.
3. The report referred to in the preceding paragraph shall, namely:
   a) describe the characteristics of the risk mapping and suspicious transaction detection system;
   b) indicate the monitoring results, i.e. alerts, transactions analyzed and reported to banking networks or agents; and
   c) indicate the transactions reported to the authorities responsible for anti-money laundering, counter-terrorism financing and financing of proliferation of weapons of mass destruction.

SECTION II

Agents

ARTICLE 118

Agent suitability

1. Money remitters and mobile money networks operating in Mozambique shall ensure the ongoing suitability of agents deployed in Mozambique.
2. For the purposes of the preceding paragraph, the institutions referred to shall lay down criteria which may eventually lead to the suspension of staff and implement an appropriate system of internal control and internal audit.

ARTICLE 119

Training

1. Money remitters and mobile money networks shall ensure that their agents undergo training.
2. Money remitters shall terminate the contracts of all agents who have not undergone training on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction for more than a year.

ARTICLE 120

Irregular transactions

Money remitters and mobile money networks shall ensure that all agents whose balance between sent and received transactions show issues, regarding the general typology of money remittance transactions provide due justification and, if need be, suspend or terminate the contracts if clarifications are not provided timely or do not prove satisfactory.

ARTICLE 121

Updated list of agents

Money remitters and mobile money networks shall keep an up-to-date list of their customers and networks within or outside Mozambique, if any, and, upon request, provide full and immediate access to the list to the competent authorities.

ARTICLE 122

Foreign agents

1. If a money remitter has foreign networks or agents, it must ensure that they apply the relevant measures consistently with requirements for Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing laid down in Mozambican laws and the rules and regulations issued in respect of such laws.
2. When the minimum requirements for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction are less stringent than those of Mozambique, or in the absence thereof, the money remitter shall apply the requirements of the Mozambican jurisdiction.

ARTICLE 123

Liability

Money remitters and mobile money networks shall be liable for all transactions processed by the agents they hire.

SECTION III

Banking networks

ARTICLE 124

Interinstitutional coordination

Money remitters and mobile money networks operating in Mozambique via bank networks shall ensure proper coordination of their risk mapping and framework of money laundering monitoring, terrorist financing and weapons of mass destruction proliferation financing with that set up by their banking counterparties for their own operations.

ARTICLE 125

Suspicious transaction search and identification criteria

Money remitters and mobile money networks shall ensure that the suspicious transaction search and identification criteria are consistent and cover all types of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

ARTICLE 126

Reporting to the Mozambique Financial Information Office

1. Money remitters and mobile money networks shall report to the GIFiM any cash transactions or mobile money transfers of amounts provided for in Article (1) of Law No. 11/2022, of July 7, or the equivalent in any other foreign currency.

2. The amount referred to in the preceding paragraph may concern a single transaction or the aggregate amount of several transactions carried out by one person, within a month.

3. In the case of mobile money, the amount referred to in the preceding paragraph may consist of the aggregate of the use or more mobile money accounts registered with the name and/or address of the same person.

ARTICLE 127

Mobile money accounts

1. Mobile money networks must be able to account for the mobile money accounts held by each customer, their particulars and the details of registration or subscription.

2. Mobile money networks may bind the accounts held by customers to the total value of transactions carried out in any time frame.

ARTICLE 128

Information provision

1. Money remitters shall provide the Banco de Moçambique with information:

a) the ownership and management structure, when comprising any involvement with PEPs; and

b) the nature of their customer base and agents;

c) the geographical areas in which it operates.

2. The information referred to in the preceding paragraph shall form part of an activity and risk report sent annually to the Banco de Moçambique by January 31.

ARTICLE 129

Management Information System

1. Money remitters shall have a proper Management Information System (MIS) in place.

2. For the purposes of this Notice, the MIS is an information system used for decision-taking, transaction processing, bookkeeping, coordination, internal control, auditing and visualizing information and the entire organization in order to complement the process of identifying and verifying customers.

3. The MIS shall regularly provide timely information in order to enable money remitters to report and detect any irregularity in transactions or any suspicious activity.

ARTICLE 130

Risk assessment

Without prejudice to the provisions in Chapter IX, money remitters shall implement an appropriate risk assessment, risk mapping and monitoring framework to monitor specific risks in their activities.

CHAPTER XIII

Specific Provisions Applicable to Microfinance Operators

ARTICLE 131

Scope

Without prejudice to the provisions in Chapters I to XI, this Chapter is applicable to credit unions, savings and loans organizations and microcredit operators and their business.

ARTICLE 132

Exemptions

Exceptionally, microfinance institutions may benefit from exemptions from certain provisions set out herein, if:

a) they have carried out a risk assessment of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, as provided by Article 134, and ascertained that risk is low;

b) their business consists in providing financial products or services appropriately set out and limited to low-risk customers, so as to increase the financial inclusion index; and

c) they are permitted by the Banco de Moçambique to apply a simplified due diligence framework to low-risk customers, with the remaining being applicable to standard due diligence measures.

ARTICLE 133

Risk assessment

1. The risk assessment should be based on a holistic approach and consider several items, including in particular the risks concerning the products and profile of low-income persons, with rather restricted or no access to financial services.

2. Microfinance operators cannot classify their customers as lower-risk solely on the grounds of them being natural low-income persons, which are set to or have recently been incorporated in the regulated financial system or are financially excluded.

3. For risks associated with the digital nature of a particular product or service, including products regarding new distribution technologies or channels by means of new technologies and services, inter alia, online banking, risk assessment shall consider the following factors:

a) the absence of in-person relationship, considering the safeguards applied;
b) geographical coverage;
c) forms of financing and access to cash;
d) the segmentation of services between the various parties for the payment execution.

ARTICLE 134

Simplified due diligence measures

1. Microcredit operators and savings and loan organizations authorized by the Banco de Moçambique may apply a simplified due diligence framework to customers whose business does not exceed the limit of 20,000.00 MT monthly and the limit of 120,000.00 MT annually.

2. For account holders, the above-mentioned microfinance operators may only apply the simplified due diligence framework if the account opened therein is the only account held by the customer in the financial system.

3. Credit unions may apply a simplified due diligence framework to customers holding a basic bank account, as provided by the specific legislation.

4. Any other customers not provided for in the previous paragraphs shall be subject to the application of standard due diligence measures.

ARTICLE 135

Simplified identification and verification framework

1. The simplified due diligence framework consists of:

a) collecting the customer's full name;
b) collecting the type and number of the customer's identification document;
c) use the Single Bank Identification Number (NUIB) in the customer's registration.

2. During the period referred to in Article 136 (2), the process of customer identification may consist of the gathering of two suitable witnesses and other possible means of customer identity proof, previously reported to the Banco de Moçambique.

3. For credit granting, the microfinance operator must take the reasonable measures in order to verify if the guarantees provided are not proceeds of crime.

ARTICLE 136

Exceptional cases

1. Microfinance operators may apply a simplified due diligence framework for individuals formally recognized as refugees and asylum-seekers in Mozambique.

2. Customers who evidently have no identification document may form business relationships with microfinance operators to open temporary accounts, which cannot be maintained more than three months.

3. As provided for in Article 16 (13) of Law No. 11/2022, of July 7, microfinance operators may not allow the carrying out of any debit or credit movements in the accounts referred to in the previous paragraph.

4. In the cases referred to in the preceding paragraph, microfinance operators shall adopt and implement a proper process of identification based on the testimonies of suitable persons or other evidence.

ARTICLE 137

Actual beneficiary

1. If the individual customer or a closely related family member does not appear to be the actual beneficiary, they should not be treated as lower risk.

2. In the cases noted in the previous paragraph, microfinance operators shall apply standard or enhanced due diligence measures, in compliance with the risk assessment associated to the case concerned.

ARTICLE 138

Exceptions

1. Microfinance operators authorized by the Banco de Moçambique to apply the simplified due diligence framework may:

a) By way of derogation from Article 29, refrain from rating retails customers;
b) as an exception to Article 30, refrain from implementing a trigger management system to assess customer acceptance;
c) as an exception to Article 35, refrain from requesting evidence for identity confirmation and verification;
d) as an exception to Article 46, refrain from collecting information about the source of income of their customers and nature of business;
e) by way of derogation from Article 47, refrain from requesting proof such as water or electricity bill, bank reference, etc.;
f) as an exception to Article 48, refrain from requesting proof of telephone, employer, economic activity, etc.; and
g) as an exception to Article 92, refrain from implementing automated profiling and information technology filtering tools to detect potentially suspicious transactions.

2. The provisions set out in the previous paragraph do not exempt
microfinance operators from

a) training all staff members;
b) laying down adapted screening, identification and investigation procedures to detect the types of high-risk transactions of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, as provided by this Notice.

CHAPTER XIV

Specific Provisions Applicable to Virtual Asset Service Providers

ARTICLE 139

Scope of Implementation

Without prejudice to the provisions of Chapters I to XI of this Notice, this Chapter applies especially to virtual asset service providers.

ARTICLE 140

Appointment of representatives

Virtual asset service providers operating in Mozambique from a foreign jurisdiction shall appoint a representative in Mozambique responsible, inter alia, for responding to requests from supervisory authorities and authorities responsible for Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing.

ARTICLE 141

Risk mapping and monitoring

1. Virtual asset service providers shall lay down a specific risk mapping for their transactions in, from and to Mozambique and apply tailored methods to identify potentially suspicious transactions.

2. Risk mapping and the characteristics of the monitoring structure referred to in the previous paragraph shall be communicated to the Banco de Moçambique by means of an annual report, in the form and within the deadlines set out by the Banco de Moçambique by Circular.

ARTICLE 142

Agents

1. Virtual asset service providers operating in Mozambique shall ensure the ongoing suitability of their agents.

2. Virtual asset service providers are liable for all transactions processed by their agents.

ARTICLE 143

Agent training

Virtual asset service providers must ensure the training of their agents on anti-money laundering, counter-terrorist proliferation of weapons of mass destruction financing.

ARTICLE 144

Contract termination

1. Virtual asset service providers shall terminate the contracts of all agents who have not undergone training on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction for more than a year.

2. Virtual asset service providers shall lay down the criteria leading up to the termination of agent contracts.

ARTICLE 145

Programs and systems

1. Virtual asset service provides must have and maintain programs and systems on Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing suitable to manage and mitigate their risks.

2. Virtual asset service providers shall have systems capable of flagging for analysis any unusual or suspicious movements of funds, transactions or activities that suggest a potential involvement in illicit activity, regardless of whether the transactions or activities are of a fiduciary, virtual-to-virtual, fiduciary-to-virtual nature or vice versa.

ARTICLE 146

Management Information System

Virtual asset service providers shall have a proper electronic MIS, as provided by Article 129 herein.

ARTICLE 147

Internal control

Virtual asset service providers shall have internal control systems comprising proper corporate governance rules that allow to:

a) strengthen control requirements for riskier situations for activities concerning virtual assets;

b) apply enhanced due diligence measure, when necessary;

c) identify, understand and assess the existing risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction concerning virtual assets;

d) identify, understand and assess the risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction concerning the financial activities or transactions of virtual assets and virtual asset service providers, centered on potentially higher-risk virtual assets; and

e) adopt measures to effectively mitigate the risks referred to in points *c)* and *d)* of this Article.

ARTICLE 148

Risk assessment and mapping

1. Risk assessment by virtual asset service providers is mandatory and considers all risk factors that those financial institutions and competent authorities consider relevant, including:

a) types of services, products or transactions, delivery channels concerned;

b) customer risk;

c) geographical factors;

d) types of virtual assets exchanged; and

e) robustness of the compliance program of virtual asset service providers.

2. In ascertaining the risk level, as provided by the previous paragraph, virtual asset service providers shall consider the extent to which users may use virtual assets or use virtual asset service providers globally to make payments or transfer funds.

3. Without prejudice to the provisions of Chapter IX herein, in addition to carrying out an appropriate risk assessment, virtual asset service providers shall implement a risk mapping and a monitoring framework to follow the specific risk to their businesses, specifically, among other potential risks, those identified in Annex VII hereto.

ARTICLE 149

Duty of identification and verification

1. Virtual asset service providers shall adopt due diligence measures whenever carrying out an occasional transaction, as set out by the requirements in Chapter VI herein.

2. When it is not possible to apply the appropriate diligence, the virtual asset service provider shall not establish a business relationship or carry out the occasional transaction and shall terminate the existing business relationship and report the suspicious transaction to GIFiM.

ARTICLE 150

Additional information

Virtual asset service providers shall collect additional information about their customers, specific to the activity, in addition to the due diligence measures required under Chapter VI herein, namely:

a) IP address (Internet Protocol) with the associated timestamp;
b) geo-location data;
c) device identifiers; and
d) virtual asset portfolio addresses.

ARTICLE 151

Enhanced due diligence measures

1. Enhanced due diligence measures shall be applied whenever a transaction is considered high risk.

2. As provided by the previous paragraph, the following, inter alia, may be considered high-risk indicators:

a) countries or geographical locations identified as funding or supporting terrorist activities or having terrorist organizations therein by credible sources;
b) countries identified as having striking rates of organized crime, corruption or other criminal activities by credit sources, including countries of origin or transit of illegal drugs, human trafficking, smuggling and illegal gambling;
c) countries subject to sanctions, bans or other similar measures issued by international organizations, such as the United Nations; and
d) countries that credible sources have identified as having poor governance, law enforcement and regulation, including countries identified by the statements of the Financial Action Task Force (FATF) as having poor anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction and to which financial institutions must pay particular attention as concerns business relationships and transactions.

3. Enhanced due diligence measures shall comprise:

a) confirm the identity information received from the customer, such as national identity number, with information in third-party databases or other credible sources;
b) screening the customer's IP address;
c) search for information available on the customer online;
d) obtain additional information from the customer about the intended nature of the business relationship;
e) obtain information about the origin of customer funds; and
f) obtain information on the reasons for the transactions intended or carried out.

ANNEX I

Risk assessment

The purpose of this Annex is to provide some examples of risk assessment. However, albeit recommended, application is not mandatory, and each financial institution shall assess the utility of this instrument in the context of its risk management policy and procedures.

I. Illustrative circumstances for risk assessment of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction:

1. The risks of money laundering, terrorist financing and financing the proliferation of weapons of mass destruction may include, but are not limited to, the following:

a) Customer risk;
b) Country or geographic risk; and
c) Risk associated with the product, services, transaction or payment channel.

2. The risk categories of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction may include, but are not limited to, the following:

a) Low risk;
b) Moderate risk; and
c) High risk.

II. Examples of different risk categories

1. **High-risk customer:**

a) The business relationship is unusual (example: a significant and unjustifiable geographical distance between the institution and the customer);
b) Non-resident customers;
c) Politically Exposed Person;
d) Legal persons or entities without legal personality structured to hold personal assets;
e) Company with shareholders on behalf of another person or bearer shares;
f) Activities that require substantial funding sources; and
g) The company's ownership structure seems unusual or overly complex given the company's business nature.

2. **Low-risk customer:**

a) Financial institutions effectively complying with requirements for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction;
b) Commercial companies listed on a stock market and subject to reporting obligations aimed at ensuring adequate transparency to actual beneficiaries; and
c) Public administrations or companies.

Note: The entities referred to in point *c*) shall not always be considered low risk.

Depending on the jurisdictions of the origin, public administrations or companies can be high risk. For example, state-owned companies originating in or operating in a country considered to have high corruption rates.

3. **High-risk country or geographical location:**

a) Countries identified by reputable sources as not having proper systems of Anti-Money Laundering, Counter Terrorist and Counter Proliferation of Weapons of Mass Destruction Financing. For example: published mutual assessment reports, detailed assessment reports or follow-up reports;

b) Countries subject to sanctions, bans or similar measures applied by the United Nations - UN (sanction by the Security Council) or other international organizations;

c) Countries identified by reputable sources as being characterized by significant levels of corruption or other criminal activity; and

d) Countries or geographical areas identified by suitable sources as financiers or supporters of terrorist activities or where designated terrorist organizations operate.

4. **Low-risk country or geographical location:**

a) Countries identified by reputable sources as not having proper systems of anti-money laundering, terrorist financing and financing of proliferation of weapons of mass destruction. For example: published mutual, detailed, or follow-up assessment reports; and

b) Countries identified by reputable sources as having low levels of corruption or other criminal activities.

5. **High risk associated with the product, service, operation or distribution channel:**

a) Private banking (corporate services, remote banking);

b) Business relationships or non-in-person customer operations; and

c) Payment received from unknown or non-associated third parties.

6. **Low risk associated with the product, service, operation or distribution channel:**

Financial products or services providing limited and appropriately defined services so as to increase access to certain types of customers for financial inclusion purposes.

ANNEX II

Ongoing due diligence measures

1. Depending on the risk category concerned, financial institutions may implement the following types of due diligence measures:

a) **Simplified due diligence measures:** less stringent due diligence measures compared to basic due diligence measures, which can only be applied when the risk is lower.

Simplified due diligence measures should be proportionate to low-risk factors.

Note: simplified measures shall not apply in cases of suspicion of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

b) **Enhanced due diligence measures:** any further due diligence measures implemented in addition to basic due diligence.

Note: all high-risk customers shall undergo enhanced due diligence measures.

2. Example of enhanced due diligence measures:

a) Obtaining additional information on customer, such as: profession, assets, information available on national or international, online and other databases;

b) Regular updating, within a maximum period of 12 months, of customer and actual beneficiary identification details;

c) Obtaining additional information about the nature of the business relationship;

d) Obtaining information of the reasons for the transactions planned or carried out;

e) Obtaining authorization from the Board of Directors or equivalent body to start or continue a business;

f) Increasing the frequency of checks and selecting the types of transactions requiring further examination; and

g) Obligation to make the first payment, through an account opened in the customer's name, from another financial institution compliant with similar due diligence standards.

3. Examples of simplified due diligence measures:

a) Verification of the identity of the customer and the actual beneficiary upon establishment of the business relationship;

b) Reducing the frequency of updates to

c) customer identification items;

d) Reducing the intensity of ongoing surveillance and

e) depth of examination and operations; and

f) Not gathering specific information or implementing specific measures to understand the subject and nature of the business relationship, but infer the subject and nature of the type of transaction carried out or the business relationship formed.

ANNEX III

Examples of suspicious transactions relating to money laundering, terrorist financing and financing of weapons of mass destruction

Notes:

A. None of the factors exemplified below, on their own, necessarily mean that a customer or third party is involved in money laundering, terrorist financing or financing of proliferation of weapons of mass destruction.

B. However, in most cases, a combination of the factors below can arouse suspicion.

C. In any case, what may or may give rise to suspicion will depend on particular circumstances.

1. Examples of suspicious money laundering transactions

1.1 Money laundering through cash transactions

a) Demand deposits in large amounts made by an individual or company that due to the type of business or activities carried out would normally be made by cheques or other instruments;

b) Substantial increases in cash deposits of any person or company, with no clear reason, especially if such deposits are then transferred within a short period

to another account and/or destination not normally associated with the customer;

c) A customer that makes several cash deposits in amounts considered normal - below the limit set out in Article 43 (3) *a*) and *b*) of Law No. 11/2022, of July 7), but which make up significant amounts in total;

d) Business accounts transactions where deposits and withdrawals are made in cash rather as movements normally associated with the business transactions of a company (for example, cheques, letters of credit, bills of exchange, etc.);

e) Customer who constantly pays or deposits money to cover requests for bank transfers, current account or other negotiable and easily tradable monetary instruments;

f) Customer who constantly requests the exchange of large quantities of low-denomination banknotes for higher-denomination banknotes;

g) Frequent exchange (purchase) of money in other currencies; and

h) Agencies/Branches with many more cash transactions than usual.

1.2 Money laundering using bank accounts

a) Customer wishing to maintain and manage a number of accounts not compatible with their business or transactions;

b) Customer who has several bank accounts and in each of them, amounts of money considered normal for their profile, but whose total balance goes beyond its financial profile.

c) Any person or company whose bank account points to a standard business profile, but is used to receive or pay large sums with no clear purpose nor relationship with the account holder and/or their business;

d) Request for payment of third-party cheques in large amounts, endorsed in favor of the customer;

e) Cash withdrawal from a previously dormant/inactive account, or from an account that has just received high credit from abroad;

f) Customer using several branches to carry out cash and foreign exchange transactions;

g) Frequent use of representatives, avoiding contact with the financial institution;

h) Substantial increases in cash deposits or negotiable instruments by a company using customer or company accounts, especially if the deposits are promptly transferred to another customer or company;

i) A customer who refuses to provide information that, under normal circumstances, would be useful for his or her eligibility for credit or other banking services.

j) Insufficient use of normal banking facilities (e.g., refusals to offer high-interest rates because of the existing balance amount); and

k) Payments made by several individuals on the same account without adequate explanation.

1.3 **Money laundering through an offshore international activity**

a) Use of letters of credit and other foreign trade financing methods to move money between countries where such trade is not compatible with the customer's usual business;

b) Customers making large payments regularly, including wire transfers, not clearly identified as bona fide transactions, or customers receiving large payments regularly from countries commonly associated with the production, processing or marketing of drugs, terrorist organizations or the practice of any of the preceding crimes referred to in Article 7 of Law No. 11/2022, of July 7;

c) Existence of large balances inconsistent with the knowledge on the customer's turnover and subsequent transfers to accounts abroad;

d) Unexplained electronic funds transfers by customers using money transfer services or similar; and

e) Frequent payments for issuing traveler's checks, withdrawals in foreign currency or other negotiable instruments.

1.4 Money laundering involving employees of financial institutions

a) Changes in employee characteristics (e.g. luxurious lifestyles)

b) Changes in the employee or agent's performance (e.g., product salesperson with noticeable or unexpected increase in performance);

c) Transactions carried out without revealing the identity of the actual beneficiary; and

d) Overbilling schemes where materials ordered for purchase are of poor quality and the prices higher than set out, with this not reflected in the negotiated contract.

1.5Money laundering using secured and unsecured financing

a) Customers repaying loans unexpectedly;

b) Financing application against assets held by the institution or a third party where the origin of goods is not reasonably known, or the goods do not match the customer's standing; and

c) Funding request with unclear repayment resources in the agreement.

1.6 Business relationship

a) Customers using the company's services for no discernible reason, such as customers with distant address who can find the same service closer to their homes;

b) Customers whose requirements do not follow the standard of the company's business, which could be more easily met elsewhere;

c) An investor introduced by a financial institution based abroad, based in countries known for drug production and trafficking, or any other crime referred to in Article 7 of Law No. 11/2022 of July 7; and

d) Any transaction where the counterparty to the operation is unknown.

1.7 Intermediaries

Any seemingly unnecessary use of an intermediary in a transaction shall give rise to an additional inquiry

1.8 Appealing to secrecy as grounds for concealing any information may arouse suspicion:

a) Excessive or unnecessary zeal of the potential customer;
b) Unnecessary granting of broad powers by power of attorney;
c) Unwillingness to disclose sources of funds; and
d) Delay and/or unwillingness to disclose the identity of actual beneficiaries.

1.9 Suspicious factors in companies' operations:

a) Companies with ongoing operations despite substantial losses;
b) Complex group structures, with no clear cause;
c) Frequent turnover of shareholders, directors or heads with no clear cause;
d) Profitable group structure for tax purposes;
e) Use of bank accounts in multiple currencies with no clear reason;
f) The existence of unexplained transfers of large sums of money, through various bank accounts; and
g) Fraudulent administration or management to the detriment of the own company's interests.

2. Examples of suspicious transactions - terrorist financing

2.1 Accounts

a) Inactive account holding a minimum balance, which suddenly receives a deposit or series of deposits, followed by daily withdrawals up to the limit of the deposited amount;
b) When opening an account, the customer eludes to provide the information required by the financial institution, or makes false or hard-to-verify statements;
c) An account on which several persons are conferred powers to sign, and said persons do not seem to have any relation with each other (no family or business ties); and
d) Account opened in the name of a legal person, an association or foundation, which may be linked to a terrorist organization showing balance movements above that declared.

2.2 Deposits and withdrawals

a) Business account where cash withdrawals are often privileged over other means of payment;
b) Deposits of large cash amounts to the account of a physical or legal person, when the apparent business activity of the individual or entity would be normally carried out by cheque or other payment instruments;
c) A combination of cash deposits and monetary instruments in an account where such transactions do not seem to be related to the normal activity of the account;
d) Several transactions carried out on the same day or on consecutive days at multiple branches of the financial institution, suggesting an attempt to mislead; and
e) Consecutive cash deposits and withdrawals in amounts below the GIFiM reporting limit.

2.3 Wire transfers

a) Bank transfers ordered in small amounts, on consecutive or intercalated days, with an apparent and evident effort to avoid submitting reports to GIFiM;
b) Bank transfer in the absence of information about the sender or the person on behalf of whom the transaction is carried out, when the inclusion of such information would be expected;
c) Use of multiple accounts, including personal, corporate, agency or charity accounts to collect funds and remit immediately or after a short time to a small number of foreign beneficiaries; and
d) Foreign exchange transactions carried out on behalf of a customer by a third party, followed by wire transfers of funds to locations with no clear business relationship with the customer or to countries considered non-cooperative.

2.4 Customer or activity characteristics

a) Address sharing by individuals involved in cash transactions, especially where the address is also a place of business and/or does not seem to correspond to the stated occupation (e.g., students, unemployed, self-employed, etc.);
b) Occupation declared by the customer incompatible with the level or type of transaction (e.g., student or unemployed individual receiving or sending a large number of bank transfers, or who makes the maximum daily cash withdrawals at multiple branches);
c) Transactions carried out by non-profit or charitable organizations, apparently without economic or logical purpose, and there appears to be no relationship between the organization's declared activity and the other parties to the transaction; and
d) Unexplained inconsistencies detected in the customer identification or verification process (e.g. in relation to previous or current country of residence, passport issuing country, countries visited, according to the passport registration, and in documents provided in order to confirm name, address and date of birth).

2.5 Transactions linked to geographical areas or countries or identified by reputable sources as providing funds or support for terrorist activities

a) Transactions concerning consecutive foreign currency exchanges within a short time frame via wire transfers to locations identified by reputable sources as non-cooperative jurisdictions;
b) Consecutive deposits, within a short time frame of wire transfers of funds especially to or through locations considered by reputable sources as non-cooperative jurisdictions;
c) The bank account that receives or order a large number of wire transfers, for which there is no apparent business or any other economic purpose, especially if said transfers are to or from jurisdictions deemed non-cooperative;
d) Use of multiple accounts to collect and channel funds to a small number of foreign beneficiaries, physical persons and companies, especially to non-cooperative jurisdictions;
e) A customer obtaining a credit instrument or engaging in commercial financial transactions with the movement of funds to or from non-cooperative jurisdictions, with no apparent logical business reasons to deal with such locations;

f) Opening financial institution accounts from non-cooperating jurisdictions; and

g) Send or receive funds via international transfers to and/or from non-cooperative locations or jurisdictions.

ANNEX IV

Types of transactions with a high-risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction

A. Cash transactions disproportionate to the customer profile

1. Unusually large cash deposits and recurring cash deposits disproportionate to the customer's activity.

2. Recurring cash deposits by different persons or entities into accounts of a particular customer for unclear purposes and with no relationship between those persons or entities and the customer.

B. Irregular or abnormal cash transactions

1. Large cash deposits transferred within a short time frame to a third party not closely related to the business of the transferring customer.

2. Recurring cash deposits at multiple branches of the same financial institution over a short time span, by the account holder or other persons.

3. Repeated funds withdrawals shortly following deposits with no clear justification.

C. Cash transactions with abnormal use of ATMs

1. Large deposits or withdrawals made at ATMs in order to avoid direct contact with the employees of the financial institution, especially if such deposits or withdrawals are incompatible with the customer's business nature.

2. Customer using multiple ATMs for simultaneous cash transactions
in the same account.

D. Abnormal money exchanges

1. Persons intent on exchanging large amounts of small banknotes for large denomination notes with no clear justification;

2. Persons intent on exchanging large amounts of damaged banknotes
for valid banknotes with no clear justification.

E. Abnormal use of accounts

1. Customers using several accounts to deposit large amounts of money over a short time frame.

2. Multiple transactions carried out from the customer's accounts at the financial institution to accounts in another financial institution, after which the funds return to the starting financial institution.

3. Debit and credit money movements made on the same within a short time frame with no clear justification.

4. The customer uses their account as an intermediary account for other parties or accounts.

F. Abnormal use of inactive accounts

1. Large deposits and cash withdrawals from inactive accounts.

2. Accounts receiving multiple deposits or cash transfers that are closed after a short time span or become stagnant.

3. Large transfers from abroad to inactive accounts.

G. Unusual use of transfers

1. Transfers of large amounts, especially those supported by instructions setting out cash payments incompatible with the customer's business.

2. Recurring transfers from different parties that have no clear relationship with the customer or those ordered by the customer to said parties.

3. Large transfers regularly hailing from areas known for specific crimes, such as drug trafficking or cultivation, or from states without effective systems for anti-money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

4. Actions taken to avoid prohibitions on applicable sanctions, such as removal, or resubmission and/or masking of sanctions in cross-border transactions.

H. Unusual reserve of credit lines

1. If the financial institution is offering documentary credit, import or export of goods whose type or value does not match the nature or scale of the customer's business or value of goods set out in the letter of credit or billing documents is significantly different from their real value.

2. Customer request, without clear justification, to change the name of the payee of the letter of credit or billing documents prior to payment;

3. Opening of several letters of credit or the negotiation through billing documents or financial counter-guarantees in a form incompatible with the customer's business.

4. Loan applications where collateral constitutes assets owned by third party, or provision of assets owned by third parties as additional collateral by borrowers, without a clear connection with them.

5. Registration of credit lines against the collateral of a financial institution operating abroad with no apparent reason.

6. Requests from a borrower customer to quickly transfer the loan amount to other financial institutions without clear purpose.

I. Unusual guarantee reserve

1. Multiple issuance of surety letters disproportional to the nature and scale of the customer's activity.

2. Letters of surety against financial guarantees incompatible with the scale of the customer's business or their previous transactions with the financial institution.

J. Unusual repayment of credit lines

1. Unusual payment terms or payment to third parties with no clear relationship to the letter of credit or billing documents.

2. Unexpected prepayment of debts by the customer or other parties, especially for defaulting customers.

K. Unusual guarantee settlements

Payee's request with no clear justification to settle surety letters soon after their issuance by the financial institution.

L. Unusual card activities

Frequently repeated withdrawals abroad of the maximum daily cash available to the card.

M. Unusual transactions in foreign currency

For foreign exchange transactions and traveler's checks, purchase or sale of foreign currency for large amounts incompatible with the customer's business.

N. No other unusual transactions

In addition to the process of filtering and identifying the above-mentioned typologies whose implementation in the automated surveillance tools of financial institutions is mandatory, financial institutions shall implement surveillance methods and tools adapted to the high-risk transactions set out in the annual risk assessment

ANNEX V

Biannual report on the risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction

Note:

The following data and responses to the semi-annual questionnaires should be reported with reference to December 31 and June 30 of each year, and must be sent to the Banco de Moçambique, in an Excel file provided by the Banco de Moçambique.

A. Quantitative data

Name of institution: ----------	
Data for the last 6 months ending in: ----------	

Returns are approved by: (Executive Director or equivalent) ----------	
Name of person in charge: ----------	Phone number: ----------
Email: ----------	
Date of submission to the Banco de Moçambique:-------	

1. Institutional file

Information regarding the financial institution		
1. If it is part of a group: (a) Group name: ---------- (b) Country of origin: ----------		
2. Number of employees		
2.a. Number of employees responsible for AMLCFT monitoring		
2.b. Number of employees trained in AMLCFT last year		
3. Number of agencies:		
4. Number of subsidiaries/ branches:		
5. Total assets - millions of meticais		

2. Risk analysis of selected products and services

2.1. Sensitive operations	Number of customers	Number of transactions	Amounts in meticais
a. Cheques paid in cash - issued by the Government or pension funds		In the last 6 months	The total value of transactions for the last 6 months
b. Cheques paid in cash - other		In the last 6 months	The total value of transactions for the last 6 months
c. Transactions abroad (cheques, documentary credits, transfers, etc.)		In the last 6 months	Total remittances issued in the last 6 months
d. Transactions from foreign countries (cheques, documentary credits, transfers, etc.)		In the last 6 months	Total remittances received in the past 6 months

2.2 Financing services	Number of customers	Amount in MT
A. Credit lines secured by cash, gold or the government Total facilities is ..... Number of customers ..... Total facilities	Number of customers according to	Total facilities is in accordance
B. Credit lines secured by other guarantees customer number	Number of customers according to	Total facilities
C. Lines of credit / installments paid in cash before maturity	Number of customers according to	Total facilities
D. Lines of credit / installments paid in kind prior to the due date	Number of customers according to	Total facilities

2.3. Private banking	Total number of customers	Deposits		Credit facilities		Off-balance sheet exposures	
		Number of customers	Amount in MT	Number of customers	Amount in MT	Number of customers	Amount in MT
Private banking services		Number of customers	Total deposits in	Number of customers	Total facilities	Number of customers	Total exposures

2.4. Bank card services	Number of cards	Number of customers	Volume of users in million MT
A. Cards issued with prepaid value	The number of issued cards is	The number of customers according to	The total value of transactions in the past 6 months
B. Other than credit and debit cards	The number of issued cards is	The number of customers according to	The total value of transactions in the past 6 months

2.5. Others		Number of customers	Number of transactions	Amount in MT
A. Cash Services	**A.** Cash deposits	Number of customers for whom the service has been provided in the past 6 months……	Number of cash deposits made in the past 6 months …… ……	Total value of cash deposits in the past 6 months.....
	B. Cash withdrawals	Number of customers for whom the service has been provided in the past 6 months……	Number of cash withdrawals in the past 6 months ……...	The total value of cash withdrawals in the past 6 months ……
B. Electronic banking services	**A.** Internet banking	Number of customers for whom the service has been provided in the past 6 months……	Number of transactions in the past 6 months …….	Total value of transactions in the past 6 months ....
	B. Phone banking	Number of customers for whom the service has been provided in the past 6 months……	Number of transactions in the past 6 months …….	Total value of transactions in the past 6 months ……
C. Wireless transfers	**A.** Outgoing transfers	Number of customers for whom the service has been provided in the past 6 months.....	Number of outgoing/ processed transfers in the past 6 months …….	Total value of transfers in the past 6 months……
	B. Incoming transfers	Number of customers for whom the service has been provided in the past 6 months……	Number of incoming transfers in the past 6 months……..	Total value of transactions in the past 6 months ……
	A. Purchase of foreign currency	Number of customers for whom the service has been provided in the past 6 months……	Number of transactions in the past 6 months.....	Total value of purchases made by the financial institution in the past 6 months.....

D. Foreign exchange transactions/operations	**B.** Sale of foreign currency	Number of customers for whom the service was provided in the past 6 months……	Number of transactions in the past 6 months …….	Total value of sales transactions carried out by the financial institution in the past 6 months ……
E. Foreign trade financing (documentary credits... etc.)		Number of customers for whom the service has been provided in the past 6 months……	Number of transactions in the past 6 months …….	The total value of transactions in the past 6 months……

3. Customer risk analysis

3.1. Services rendered to account holders (it is necessary to indicate the balance at the end of the period)	**Total number of customers**	**Average transactions in MT**
At the date of the report		
Total customers with accounts		
A. Individual resident customers		
B. Resident legal entities		
C. Individual non-resident customers		
D. Non-resident legal entities		

3.2. Customer risk analysis (balance required at the end of the period)	**Total number of customers**	**Average transactions in MT**
1. Non-profit entities and organizations		
a. Location		
b. Foreign		
2. Political people who pose a risk		
a. Location		
b. Foreign		
c. International organizations		
3. Private banking customers		
4. Customers dealing with cash intensively (cash inflows or outflows > 500,000 MZN/month)		
5. Legal entities / the true beneficiary is unknown		
6. Money remitters		
7. Foreign exchange bureaus		
8. Real estate business (includes agents)		
9. Dealers in gems and precious metals		
10. Business owners and non-financial professions (lawyers, accountants and intermediaries working for in favor of others)		
11. Legal entities		
a. Location		
b. Foreign		
12. Vehicle dealers and resellers, casinos and entities exploiting social and amusement games, microfinance entities		

3.3. Geospatial Risk Analysis - Analysis based on the Customer's Residence									
Clause	**Number of ATMs**	**Deposit**		**Transfers**					
				Incoming			**Outgoing**		
		Number of customers	**Deposit in MT**	**Number of transactions**	**Number of customers**	**Amounts in MT**	**Number of transactions**	**Number of customers**	**Amounts in MT**
1. Venue									
A. Border, conflict and mining zones		Number of customers according to	Total balance according to	Total number of remittances in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months	Total remittances sent in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months
B. Other regions in Mozambique		Number of customers	Total balance.....	Total number of remittances in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months	Total remittances sent in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months
2. Abroad									
A. Countries classified by the FATF as high-risk countries		Number of customers according to	Total balance according to	Total number of remittances in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months	Total remittances sent in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months
B. Other countries identified as having high risks of money laundering and terrorist financing		Number of customers according to	Total balance according to	Total number of remittances in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months	Total remittances sent in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months
C. Other countries		Number of customers according to	Total balance according to	Total number of remittances in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months	Total remittances sent in the last 6 months	Number of customers for whom the service has been provided in the last 6 months	Total value of domestic remittances in the past 6 months

Reports of unusual suspicious transactions

Clause	Number (past 6 months)
Number of unusual / suspicious operations detected	
Number of suspicious transactions reported to the GIFiM	
Number of castrated (aborted) transactions	

Qualitative questionnaires

Questions about risk assessment and profile
1. The institution has completed, during the last year, a formalized and documented risk assessment for all risks of money terrorist, terrorist financing and financing of proliferation of weapons of mass destruction?
2. If requested by the competent authorities, is the institution in a position to present a formally documented risk assessment and show the basis of the risk assessments?
3. When drawing up the risk assessment, the risk assessment methodology requires the institution to use internal information, such as operational and transactional data, as well as external information, such as national risk assessment reports?
4. Does the institution ensure that the institution's risk assessment is drawn up using both quantitative and qualitative details and is always kept up to date?
5. Does the risk assessment cover all products and services supplied and provided to customers?
6. The risk assessment considers the specifics of all transactions of the institution (nature, complexity, etc.)?
7. Does the risk assessment consider all direct and indirect distribution channels?
8. Does the risk assessment consider characteristics of customers?
9. Does the risk assessment consider the geographical areas of customers or related transactions?
10. Risk assessment considers all jurisdictions with which the institution operates, through all types of possible transactions: documentary credits, correspondent banks, transfers, etc.?
11. Has the institution integrated the factors or risks of financing terrorism and financing the proliferation of weapons of mass destruction into the risk assessment?
12. Has an internal or external event during the past year triggered a change or review of the institution's exposure to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks and subsequently led to a review of the institution's risk rating or risk assessment? *Triggering events may include, but are not limited to changes in the National Risk Assessment, changes in the shareholder structure of the institution, changes in the key control structure, negative media or reputational risks, major changes in current activities and follow-up audits of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.*
13. Have any audit missions undertaken by internal or external auditors in the last year highlighted the relevance of the institution's risk profile to money laundering, terrorist financing and financing of proliferation of weapons of mass destruction and the absence of the need to update or modify it?
14. Has the board of directors or equivalent body approved, during the past year, the risk assessment of the institution and ascertained the level of risk of money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction that the institution is ready to accept?
15. The Board of Directors of the equivalent body formally approved the risk assessment and mitigation measures adapted to the aforementioned risk level?
16. Does the Board of Directors or equivalent body ensures the monitoring of the implementation of the mitigation measures approved regarding the risk assessment?
17. Does the institution identify and assess the risks of money laundering, terrorist financing and financing of proliferation financing of mass destruction that may arise in the development of new products and new business practices, including new delivery mechanisms, the use of new or developing technologies for both new and pre-existing products?

Questions about the organization of the framework on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction
1. Has the institution organized centralized coordination in order to analyze unusual transactions detected?
2. Has the institution set up a centralized coordination to draw up reports on suspicious transactions for transactions providing for suspicion that they are of illegal origin?
2. Has the institution set up a centralized coordination to draw up reports on suspicious transactions concerning terrorist financing?
4. Has the institution set up a centralized coordination for responding to judicial or administrative requests, as well as GIFiM reporting duties?
5. Has the institution implemented automated, real-time tools and risk-based procedures to determine whether to transfer, reject or suspend transactions that are not supported by the necessary payer and payee information?
6. When outsourcing for operational activities comprising or connected to obligations regarding money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, especially if they are carried out abroad, does the institution check if the procedures are actually implemented by the service provider?
7. If the financial belongs to a group or is the parent company of a financial group, the group's procedures shall allow and facilitate the sharing of information within the group for the purposes of organizing and monitoring money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, including the forwarding of information to the group's parent company?
8. If the institution is the parent company of a financial group, does the person responsible for implementing policies on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction for the group ensures that the measures applied on entities abroad are at least equivalent to the measures in force in Mozambique?
9. If the institution is the parent company of a financial group, does the person responsible for implementing the group's legal framework on money laundering, terrorist financing and financing proliferation of weapons of mass destruction ensure that subsidiaries and branches in another state comply with the provisions applicable in that State?
10. If the institution is the parent company of a financial group, is the person responsible for implementing the group's system kept informed of suspicious transaction reports made to a Financial Reporting Unit by an entity of its group?
11. Does the institution have agencies or branches abroad whose locally applicable law prevents the parent company of the group's device from having access to the documents or transaction details?

Questions about customer due diligence
1. Does the institution ensure the identification and verification of the identity of the customer or, where applicable, the identification and verification of the identity of the actual beneficiary, irrespective of the amount of each individual transaction?
2. The institution's Customer Due Diligence (CDD) process ensures the collection and safekeeping of the following information: *a)* Ownership structure; *b)* Customer identification; *c)* Expected activities; *d)* Nature of business/employment; *e)* Requested products; *f)* Purpose of the account/ business relationship; *g)* Sources of funds; *h)* Sources of wealth; *i)* Actual beneficiaries; *j)* Geographical exposure; *k)* Type of business / industry; *l)* Products used; *m)* Type of legal entity; *n)* Information on the professional, economic and financial situation of customers?
3. If the verification of the identity of the customer and, where applicable, of the actual beneficiary, or the collection of information on the subject and nature of the business relationship proves impossible or limited, shall the institution refrain from entering into the business relationship?
4. If the verification of the identity of the customer and, where applicable, the actual beneficiary, or the collection of information on the subject and nature of the business relationship proves impossible or limited, shall the institution refrain from entering into the business relationship?
5. Does the institution have in operation a system for computing profiles and monitoring the commercial relationship?
6. Does the institution have internal procedures in place that demand that any person intending to act on behalf of a customer is authorized to so, and identify and verify said person's identity?

Questions about customer due diligence
7. Do the procedures allow the institution to detect Politically Exposed Persons (PEPs) or persons/entities related to them or associates when initiating a business relationship and during the business relationship. Moreover, does your organization investigate the origin of funds and sources of wealth of the PPE or persons/entities related to them or associates?
8. Do your procedures provided for the implementation of additional surveillance/ enhanced measures when the business relationship, product or operation has a "high risk" rating?
9. If the institution uses one or more third parties to enter into business relationships with customers, does it remain solely liable for completing due diligence for customers introduced by the third-party presenter?
10. Does the institution have a policy of updating customer information at least once a year for all customers, regardless of risk rating?
11. Does the institution have a policy of updating customer information at least once a year for all customers, regardless of risk rating?
12. Does the institution have a proper threshold management system that allows the institution to carry out the necessary CDD reviews amid any trigger event against the customer, and that may entail a customer risk rating review?
13. Do all customers on the institution's records have an appropriate risk rating?
14. Does the institution undertake terrorist actions/sanctions, negative news and customer onboarding PEP screening, and later regularly, with potential games that are timely reviewed and scaled?
15. The institution's policies and procedures clearly set out what customers and related parties require screening and how this process shall be carried out?

Questions about ongoing monitoring
1. Does the institution have automated tools to detect unusual or suspicious transactions?
2. Does the institution set importance criteria for detecting unusual and suspicious transactions, through transaction monitoring solutions or by other means, such as employee referrals?
3. If the customer does not provide a justification on the details of any specific transaction or banking activity, do the institution's policies and procedures require registration, reporting to GIFiM and/or restriction or termination of business relations with such customers?
4. Do internal procedures provided that outgoing funds transfers are accompanied by the necessary information about the payer and payee?
5. Has the institution implemented a process for the automatic detection of missing payer and payee information and risk-based procedures to determine whether to transfer, reject or suspend transactions not supported by the necessary payer and payee information?
6. Does the institution use agents and/or distributions for some of their products and they undergo regular training and guidance on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction tailored to their activities?
7. Do the institution's internal policies and procedures ensure that agents and/or distributors undergo CDD and are compliant with its framework of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction?
8. If the institution uses or is carrying out an activity in the capacity of cross-border banking correspondent, did it take all necessary measures to ensure ongoing enhanced control of such type of transactions?
9. Does the institution implement additional ongoing monitoring measures for customers or transactions deemed "high risk"?
10. For mobile money, do the institution's procedures provide for the verification of the customer's identity, regardless of the amount used to top up the account with physical money?
11. For mobile money, does the institution's system provide for the implementation of surveillance measures during the repayment and/or withdrawal of mobile money above a specific threshold set out in procedures?
12. For mobile money, do the institution's procedures comprise the collection and storage of information and technical data concerning the activation, top up and use of mobile money via a physical means for screening purposes?

Questions about the GIFiM report
1. Does the institution undertake to provided the GIFiM with potential suspicious or suspicious activity reports as part of an ongoing process of investigation, documentation, suspicious activity monitoring, whilst complying with the high accuracy and comprehensiveness standards and submitting the reports within the legal deadlines?
2. Does the institution have risk-based monitoring policies, procedures and processes for identifying and reporting unusual or suspicious activity?
3. The institution's system provides for suspicious transaction reports to include the analysis items that led to the reporting of the transactions/activities and be accompanied by any useful document for follow-up?
4. The institution's procedures include provisions on the confidentiality of the existence, content and monitoring of suspicious transactions in order to avoid "tipping off"?
5. The institution's policies and procedures require all activities determined suspicious and scaled-up be reviewed by a senior contributor and reported to the GIFiM in a timely manner?

Question on internal auditing and control
1. Does the institution have an internal audit function and an internal control function or other independent third-party to assess the risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction and the concerning related policies and practices regularly?
2. Does the Board of Directors of the institution ensure that the scope and methodology of the audit are appropriate to the risk profile of the institution, and that the frequency of such audits is also based on risk?
3. Are all adverse internal and external audit findings duly scaled-up to senior management within the formal governance framework?
4. Does the audit and/or internal control function ensure that compliance with money laundering, terrorist financing and financing of proliferation of weapons of mass destruction procedures are properly implemented in all branches and subsidiaries of the institution?
5. Does the independent audit and / or control cover third parties and agents acting on behalf of the organization to ensure compliance with the institution's policies and procedures on.money laundering, terrorist financing and proliferation of weapons of mass destruction?
6. In particular, the independent audit and/or control reviews the CDD, the enhanced due diligence process and the “Know Your Customer” process carried out for business relationships, particularly those deemed high risk by your organization?

Question on internal auditing and control
1. Does the independent audit and/or control specifically check the enhanced due diligence applied for products, services or distribution channel, especially for high-risk cases?
2. In particular, does the independent audit and/or control check the enhancement of due diligence for activities carried out with persons determined in States or territories deemed high-risk or those where the existence of strategic deficiencies are known for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction?
3. Does the independent audit and/or control check the regular updating of the knowledge details (CDD) of the business relationship according to the frequency set out in the procedures and adapted to the risks?
4. Does the independent audit and/or control check the diligent handling of alerts on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, and whether the alerts generated are dealt with promptly and closed with a proper risk assessment?
5. Does the internal audit verify, in particular, the relevance of the rating of risks of money laundering and terrorist financing and financing of proliferation of weapons of mass destruction drawn up by the institution?
6. Does the internal audit and/or control verify the adequacy of the institution's policies and procedures on anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction in addressing the risks identified?
7. Does the internal audit and/or control check in particular the effectiveness of the institution's personnel in implementing the institution's policies and procedures; especially, the system for detecting and analyzing operations of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction?
8. Does internal audit and / or control test the effectiveness of training on money laundering, terrorist financing and financing of proliferation of weapons of mass destruction of relevant institution employees?
9. Is the date of the last audit mission carried out by the full or partial internal audit of the institution's system of anti-money laundering, terrorist financing and financing of proliferation of weapons of mass destruction less than one year?
10. Does the internal audit check the controls to the configuration of systems of anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction, the situations and sufficiency of situations deployed?
11. Independent audit/control functions review asset freeze practices to ensure implementation, following entry into force, of measures freezing funds or economic resources?
12. Independent audit/control functions review practices related to onboarding name screening, name screening throughout the relationship and CDD review, transaction screening and sanction list management?

Questions about ongoing monitoring
1. The Board of Directors or equivalent body and top management are actively involved in the implementation of a sound compliance framework that protects the institution against any risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction or sanctions?
2. Is risk management integrated into three lines of defense where the second line of defense includes the head of operations responsible for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction, as well as the compliance function and the third line of defense is ensured by the internal audit function?
3. Does the Board of Directors and management formally report the tolerance to risk and strategies of risk acceptance of the institution to all institution employees?
4. Has the Board of Directors or equivalent body made recommendations to all institution staff members on the implementation of the policy on anti-money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in the last year?
5. Is there a suitably qualified officer appointed by the Board of Directors who is mainly responsible for the duties of anti-money laundering, terrorist financing or financing of proliferation of weapons of mass destruction?
6. Has the institution implemented a formal governance structure where top management committees and subcommittees are responsible for compliance with anti-money laundering, counter-terrorist financing and financing of proliferation of mass destruction also receive reports on all major issues of compliance with mitigation measures?
7. Is satisfactory information regularly provided to committees and subcommittees?
7.1. The agendas of the committees should normally address issues of risk of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction and sanctions, mitigation plans for deadlines for closures, including provisional controls;
7.2. The committees should also oversee the types of money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction, new risk trends, statistics and any regulatory concerns.
8. The Board of Directors or equivalent body has recommended ceasing or avoiding entering into business relations with customers for whom due diligence has not given full assurance of legitimacy?
9. Has the Board of Directors approved an escalation process to directly examine specific customer cases whose business relationship may comprise money laundering, terrorist financing and financing of proliferation of weapons of mass destruction matters

Questions about compliance
1. The institution has procedures/plans in place to raise the awareness of staff members to the risks of money laundering, terrorist financing and financing of proliferation of weapons of mass destruction?
2. Is training on anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction covering all risks provided to the Board of Directors, management, the first, the second and the third line of defense and third parties to whom specific activities have been outsourced mandatory?
3. Does the institution provide mandatory training on anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction when the staff are recruited and to all staff on an annual basis?
Is all personnel required to pass a test at the end of training with a minimum grade of completion?
5. If an employee fails the test, are there follow-up measures clearly documented in the institution's policies and procedures?
6. Are all agents and persons acting on behalf of and in the name of the institution, in contact with customers, informed and trained, at least annually, on specific risk factors for money laundering, terrorist financing and financing of proliferation of weapons of mass destruction, including operational procedures for carrying out the tasks concerning their function?
7. Are all agents and persons acting for and in the name of the organization in contact with customers informed and trained at least annually on specific risk factors for terrorist financing, including operational procedures for carrying out the tasks concerning their function?
8. Are specific steps taken in order to ensure the suitability and predisposition of the agents responsible for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction?
9. Has the Board of Directors or equivalent body decided on specific provisions on the prevention of conflicts of interest for staff responsible for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction?
10. The board has set up the function on anti-money laundering, counter-terrorism financing and financing of proliferation of weapons of mass destruction with all relevant provisions so as to ensure independence (remuneration, organizational chart position, hierarchical reporting, etc.)?

Questions about specific matters
1. The institution allows to detect, following the coming into effect of a new national measure or sanctions by the United Nations (UN), such as asset freezing, any sum or transaction that might be concerned?
2. Does your organization allow detecting, following the implementation of a new national measure or UN sanctions (such as asset freezes), funds and economic resources that do not belong to a person or entity subject to an asset freeze, but controlled by it?
3. If an institution has an automated computer filtering tool, do you consider the spelling variations of the names and surnames of these persons or entities that would not correspond exactly to those lodged in national and UN sanctions lists?
4. The institution's monitoring system allows for detecting cash transactions disproportionate to the customer's profile: *a)* Exceptionally large cash deposits and recurring cash deposits incompatible with the customer's business; *b)* Recurring cash deposits by various persons or entities into accounts of a particular customer for unclear purposes and without any relationship between such persons or entities and the customer.
5. Their monitoring system allows to detect cash transactions with irregular or abnormal characteristics: *a)* Large cash deposits that are transferred, in a short time frame, to a third party not closely related to the activity of the transferring customer; *b)* Recurring cash deposits at multiple branches of the same institution in a short timeframe, by the account holder, or other small repeated withdrawals of funds shortly following deposit, with no clear reason.
6. The institution's internal control system allows detecting cash transactions with abnormal use of ATMs: *a)* Large deposits or withdrawals at automated teller machines to avoid direct contact with the institution's staff, especially if such deposits or withdrawals are not compliant with the customer's business nature; *b)* Customer using multiple ATMs for simultaneous cash transactions on the same account.
7. The institution's monitoring system allow for detecting abnormal money exchanges: *a)* Persons seeking to exchange large amounts of small face value banknotes for large face value banknotes with no clear justification; *b)* Persons seeking to exchange large amounts of damaged banknotes for valid banknotes with no clear justification.
8. The institution's control system allows for detecting abnormal use of accounts: *a)* Customers using multiple accounts to deposit large amounts of money in a short time frame; *b)* Multiple transactions made from the customer's accounts at the institution to accounts at another institution, where said funds return to the starting institution; *c)* Cash debit and credit movements made to the same account in a short time frame with no clear justification; *d)* The customer uses their account as an intermediary account for other parties or accounts.
9. The institution's monitoring systems allow detecting the abnormal use of inactive accounts: *a)* Large deposits and cash withdrawals from inactive accounts; *b)* Accounts receiving multiple deposits or cash transfers, but are then closed after a short time frame or left stagnant; *c)* Large transfers from abroad to inactive accounts.
10. The institution's monitoring system can detect the unusual use of transfers: *a)* Transfers in large amounts, especially those accompanied by cash payment instructions incompatible with the customer's activity; *b)* Recurring transfers from different parties with no clear relationship with the customer or those that are sent by the customer to those parties; *c)* Large transfers regularly hailing from areas known for specific crimes, such as drug trafficking or cultivation, or from states without effective systems for anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction; *d)* Measures taken to circumvent the prohibitions of applicable sanctions, such as the removal, or re-submission and/or masking of relevant information in cross-border transactions.
11. The monitoring system detects unusual credit facility reserves: *a)* If the institution offers documentary credit, import or export of goods whose type or value does not match the nature or size of the customer's business or the value of the goods indicated in the letter of credit or billing documents differs significantly from their real value; *b)* Customer request with no clear justification to change the name of the payee of the letter of credit or billing documents prior to payment; *c)* Opening of several credit letters or negotiation through billing documents or financial counter-guarantees in a form incompatible with the customer's business; *d)* Loan applications by securing assets belonging to third parties, or by providing additional guarantees by part of borrowers, with no clear connection to these; *e)* Reserve of credit facilities against the guarantees of an institution operating abroad with no clear reason; *f)* Requests from a borrower customer to quickly transfer the loan amount to other financial institutions with no clear purpose.

Questions about specific matters
12. The institution's monitoring system allows it to detect unusual guarantee reserves, such as: *a)* Multiple issuance of letters of guarantee, incompatible with the customer's business nature and size; *b)* Letters of guarantee, financial counter-guarantees not proportional to the size of the customer's business or its previous transactions with the institution.
13. The institution's monitoring system allows it to detect the unusual repayment of credit facilities, such as: *a)* Unusual payment terms or payment to third parties with no clear relationship with the letter of credit or billing documents; *b)* Unexpected early payment of debts by the customer or other parties, especially defaulting customers.
14. The institution's monitoring system allows it to detect unusual collateral settlements such as: *a)* Request by the payee with no clear reason to settle letters of guarantee shortly after issuance by the institution.
15. The institution's monitoring system allows it to detect unusual card activities such as: *a)* Frequent repeated withdrawal of the maximum daily money available for the card.
16. The institution's monitoring system allows it to detect unusual foreign currency transactions such as: *a)* Foreign exchange transactions and traveler's cheques, purchase or sale of foreign currency for large amounts incompatible with the customer's business.

ANNEX VI

Risk assessment specific to the business of money remitters and mobile money networks

1. Customer categories

***a)* Categories of customers whose business or activities may suggest a higher risk, including:**

i. Agents representing more than one money remitter;

ii. Agents in a high-risk jurisdiction or country or dealing with high-risk customers or transactions;

iii. Agents carrying out an uncommon and high number of transactions with another agent location, especially with an agent in a high-risk geographical area or broker customers or transactions;

iv. The agent's volume of transactions is inconsistent with the global volume or standard volume of previous transactions;

v. Transaction pattern suggesting the value of transactions immediately below any applicable due diligence limit;

vi. Agents who have received negative attention from credible media or sanctions from law enforcement authorities;

vii. Agents who did not attend nor complete training.

viii. Agents operating below-standard compliance programs, comprising programs that do not effectively manage compliance with internal policies, external regulation, etc.;

ix. Agents with a history of regulatory non-compliance and unwilling to follow the review recommendations of the compliance programs and subject to suspension or termination;

x. Agents who do not provide the necessary information on the originator of the transfer upon request.

xi. Agents whose data collection or keeping of records is negligent, careless or inconsistent;

xii. Agents willing to accept false identification or identification records containing false information, non-existent addresses that would be known to be non-existent to a person in said area, or false or non-existent telephone numbers used as fill-ins;

xiii. Agents with an unbalanced send-to-receive ratio, consistent with other agents in the location, or whose transactions and activities indicate potential complicity with criminal activity;

xiv. Agents whose seasonal fluctuation of business is incompatible with their income or with other agents on the location, or is compatible with criminal procedure standards; and

xv. Agents with a suspicious or irregular proportion of customers, given that they are not part of normal groups for the places where they operate or those similar.

***b)* Categories of customers whose business or activities may indicate a higher risk,** including:

i. The customer or counterparty is a money remitter or financial institution that has been sanctioned by the concerning competent national authorities for not complying with the framework for anti-money laundering, counter-terrorist financing and financing of proliferation of weapon of mass destruction and is not engaged in carrying out corrections so as to improve compliance.

***c)* Customer carrying out their business relations or transactions in unusual circumstances,** such as:

i. The customer travels unreasonable distances to distant locations to carry out transactions;

ii. Customer networks (i.e., defined groups of individuals transacting at one or more points of sale, or across multiple services);

iii. The customer owns or runs a cash-based business suggestive of a fake or shell company, or combines illicit and lawful earnings, as provided by a screening of transactions that appear inconsistent with the financial standing or occupation;

iv. Politically Exposed Persons, their family members or close associates, and where the actual beneficiary of a customer is a politically exposed politician, as provided for in FATF recommendation 12;

v. Non-in-person customer, when doubts regarding identity exist;

vi. Customer using agents or associates where the nature of the relationship or transaction makes it difficult to identify the actual beneficiary of the funds;

vii. Customer completely unaware or reluctant to disclose payee details, such as address, contact information, etc.;

viii. Customer providing inconsistent information (e.g., giving different names);

ix. Customer involved in transactions with no clear ties with the country of destination with no reasonable explanation;

x. A customer who has been sanctioned by the law enforcement authority, regarding proceeds generating crimes, known by the money transmitter;

xi. Customer providing false or fraudulent identification, whether evidenced by the document alone, by the document's lack of connection to the customer, or by the document's context with other documents (e.g., use of identification cards or documents in different names without reasonable explanation); and

xii. Customer whose transactions and activities indicate connection to potential criminal involvement, types or "red flags" provided in reports produced by the FATF or competent national authorities, such as the GIFiM and law enforcement authorities.

d) Suspicion that the customer is acting on behalf of a third party, but does not disclose this information, or is being controlled by another person (their handler). For example: the customer takes a money transfer and immediately hands it over to another person, or another person requests the customer to make a transfer, but they make the transaction in their name.

2. In addition to the situations provided for in the preceding paragraph, money remitters shall consider other high-risk situations related to their business, which may, for example, include, attempted or sent transactions, whilst considering the following sample cases:

a) **Point of origin customer behavior:**

i. The customer structures the transaction seemingly so as to attempt to split the amounts in order to remain below any applicable due diligence limit, and avoid reporting or record keeping;

ii. The transaction is unnecessarily complex with no apparent commercial or legal purpose;

iii. The number or amount of transactions is inconsistent with the financial standing or occupation or is outside the normal course of business of the customer in light of the information provided by the customer when carrying out the transaction, or during subsequent contact (such as an interview, discussion or based on the information provided to the tax authorities and made available to the money remitter.);

iv. The customer offers an unusual bribe or tip, or is willing to pay unusual fees to carry out transactions;

v. The customer has vague knowledge about the amount of money concerning the transaction;

vi. The customer asks unusual questions, threatens or tries to convince staff members in order to avoid reporting;

vii. The customer sends money internationally and expects to receive an equal transfer or vice versa;

viii. The customer transfers money to illegal online gambling sites or the existence of email address with references to gambling of transfers to countries with a high number online gambling sites is verified;

ix. The customer transfers money to a higher risk jurisdiction, country or corridor;

x. The customer attempts a transaction, but since they would likely undergo due diligence measures due to the amount, they cancel the transaction in order to avoid reporting or other requirements;

xi. The customer transfers money in order to claim lottery prizes or other prizes to someone they have only met online;

xii. Transfers to credit cards for loan fees, job opportunities or mysterious purchasing opportunities are indicators of potential consumer fraud; and

xiii. Payers appear to have no family ties with the payee and no grounds for the transfer.

b) Activity detected during monitoring, where in many of the situations customer activity may be apparent both during interaction at the point of sale and during back-end transaction monitoring of , such as:

i. Transfers to the same person from different persons or to different persons from the same person with no clear justification;

ii. Unusually large, high volume, or frequency of transactions for no logical or clear reason;

iii. The customer uses nicknames, pseudonyms or several different names and addresses;

iv. . Customers with a concentration rate of transfers made to a jurisdiction notably higher than expected considering the global customer base;

v. Customers transferring or receiving funds from persons involved in criminal activities, in light of available information;

vi. Customer network that uses shared contact information, such as address, phone, or email, where such sharing is not normal or reasonably justifiable; and

vii. Transfers to HOSSPs in locations where such transactions are considered illegal by the money remitter.

***c)* Incoming transactions:**

i. Transactions not supported by the required payer or payee information;

ii. Situations where additional customer or transactional information was requested from a requesting money remitter, but was not received; and

iii. Large number of incoming transactions at once, or during a certain period of time, which do not seem to correspond to the usual past pattern of the payee (for example: during the seasons of production of illicit drugs, for smuggling migrants, etc.).

ANNEX VII

Risks specific to the business of virtual asset service providers

Providers of virtual asset services should monitor the specific risks of their business specifically, among other potential, the following:

1. Volume and frequency of transactions, including:

a) Structuring of virtual asset transactions in small amounts or amounts below registration or reporting limits;

b) Carrying out several high-value transactions in a short timeframe, in a phased and regular pattern, with no new transactions recorded, over a long period afterwards either for a newly created account or for a previously inactive account;

c) Transfer of virtual assets immediately to multiple virtual asset service providers;

d) Deposit of virtual assets on an exchange and often subsequent withdrawal and immediate conversion into several types of virtual assets or withdrawal of assets from a virtual asset service provider directly into a private portfolio; and

e) Accepting funds suspected of being stolen, embezzled or fraudulent.

2. Red flags on transaction patterns, including:

a) Transactions concerning large initial deposits, referring to new users, inconsistent with the customer's profile;

b) Transactions of new users concerning a large initial deposit and total funding of the deposit during the first day, and the customer starts trading the full or a large part of the amount in the same or the next day or the customer withdraws the full amount the next day;

c) New user trying to trade the entire balance of virtual assets; and

d) New user who withdraws the virtual assets and attempts to send the entire balance out of the platform.

3. Transaction of users, which may concern the principle of "no justifiable business logic", including:

a) Use of multiple virtual assets;

b) Use of multiple accounts;

c) Frequent transfers in a specific timeframe, namely, day, week, month, etc.;

d) Incoming transactions from several unrelated portfolios, in relatively small amounts, with subsequent transfer to another portfolio or full exchange for fiat currency;

e) Converting fiat currency into virtual assets, with potential loss;

f) Converting a large amount of fiat currency into virtual assets;

g) Converting a large amount of one type of virtual asset into other types of virtual assets.

4. Red flags on anonymity, including:

a) Despite the additional transaction fees, more than one type of virtual asset is involved, especially if they provide greater possibility of anonymity.

b) Movement of a virtual asset operating on a public and transparent blockchain to a centralized exchange service and then immediate exchanged for a *privacy coin'* or Anonymity-Enhanced Cryptocurrencies (AEC);

c) Customers operating as an unregistered or licensed virtual asset service provider on online peer-to-peer (P2P) exchange sites;

d) Abnormal transactional activity of virtual assets withdrawn from associated with the P2P platform;

e) Virtual assets transferred to and from portfolios with past activity patterns associated with the use of virtual asset service providers operating mixed services or P2P platforms;

f) Use of "mixing and tumbling services";

g) Funds deposited or withdrawn from an address or virtual asset portfolio with direct and indirect exposure links to known suspicious sources;

h) Use of decentralized or unallocated hardware or paper portfolios to transport virtual assets cross-borders;

i) Users of the virtual asset service provider platform who register their domain names on the internet through proxies or using a Domain Name System (DNS) that suppress or eliminate the owners of domain names;

j) Users of the virtual asset service provider platform using an IP address associated with darknet or other similar software that allows anonymous communication;

k) Transactions by anonymous encrypted means of communication rather than a virtual asset service provider;

l) Existence of a large number of seemingly unrelated virtual asset portfolios controlled from the same IP address or Media Access Control (MAC) address;

m) Use of virtual assets whose design is not properly documented;

n) Use of virtual assets linked to possible fraud or fraudulent schemes;

o) Receiving or sending funds to virtual asset service providers with weak or non-existent Know-Your-Customer processes;

p) Use of ATMs or digital virtual asset kiosks despite higher transaction fees, including those commonly used by money mules or victims of fraud or scams, especially in high-risk locations where greater criminal activities take place.

Note: only using one ATM shall not necessarily make for a red flag, unless the ATM is in a high-risk area or is used for small repeated transactions or other additional factors.

5. Payer or payee red flags, including:

a) During account creation:

i. Creating separate accounts with different names;

ii. Transactions initiated from untrusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious;

iii. Attempting to open an account frequently with the same virtual asset service provider from the same IP address; and

iv. Merchants or business users with internet domain registrations in a jurisdiction other than the jurisdiction of establishment or in another with a weak domain registration process.

b) During the enhanced due diligence process:

i. Incomplete or insufficient ”Know Your Customer" Information or customers who refuse requests for related documents or inquiries about the origin of funds;

ii. Transactions unbeknownst to the payer, payee or when unclear information about the transaction, source of resources or relationship with the counterparty are provided; and

iii. Customer providing forged documents or edited photographs as part of the onboarding process.

c) Customer profile:

i. The customer provides identification data or account credentials shared by another account;

ii. IP addresses associated with the customer profile different from the IP addresses starting the transactions;

iii. The customer's virtual address shows up in public forums associated with illegal activities;

iv. The customer is known through publicly available information due to previous criminal association; and

v. Customer profile does not match trading of high-value virtual assets.

d) Potential money mule profile or victim of scam:

i. The sender is not acquainted with virtual assets technology or online escrow wallet solutions;

ii. The customer is much older than the average users that open accounts on the platform and carry out several transactions;

iii. Financially vulnerable customer; and

iv. The customer procures large amounts of virtual assets, unfounded on the wealth available or inconsistent with their historical financial profile.

6. Other unusual behaviors, including:

a) Customers who frequently change the identification information, such as e-mail addresses, IP addresses, financial information, etc.;

b) Customers who attempt to log in to the platforms of one or more virtual asset service providers using different IP addresses frequently on the same day;

c) Use of language in virtual asset message fields indicative of transactions supporting illicit activity or purchase of illicit goods; and

d) Customers who repeatedly transact with a subset of individuals for significant profit or loss.

7. Red flags on source of funds or wealth, including:

a) Transactions with virtual asset addresses or bank cards linked to known fraud, extortion schemes, ransomware, sanctioned addresses, darknet markets or other pages of illicit websites;

b) Transactions in virtual assets originating in or destined for online gambling services ;

c) Use of one or several credit or debit cards associated with a virtual asset portfolio to withdraw large amounts of fiduciary values;

d) Resources to purchase virtual assets from cash deposits on credit cards;

e) Account deposits or virtual asset address significantly larger than normal, with an unknown source of funds, followed by conversion to fiat currency;

f) Lack of transparency or sufficient information on the origin and holders of funds;

g) Incoming transactions of online payment systems via credit cards or prepaid, followed by instant withdrawal;

h) Funds directly from mixed third-party services or portfolio;

i) Much of a customer's source of wealth derived from investments in virtual assets, fraudulent Initial Coin Offering, etc.; and

j) Source of customer wealth unevenly drawn from virtual assets from other providers of virtual asset services that do not have controls for anti-money laundering, terrorist financing and financing of proliferation of weapons of mass destruction.

8. Payer or payee red flags, regarding geographical risks, including:

a) Customer funds originate from or are sent to a wallet not registered in the jurisdiction where the customer or the exchange is located;

b) Customer using a virtual asset exchange or funds transfer institution located in a high-risk jurisdiction

with inadequate anti-money laundering, terrorist-financing and financing of proliferation of weapons of mass destruction regulations for virtual asset service providers and inadequate due diligence or "Know Your Customer" measures;

c) Customer sending funds to virtual asset service providers operating in jurisdictions lacking a virtual asset regulation or not implementing anti-money laundering, counter-terrorist financing and financing of proliferation of weapons of mass destruction control;

d) Customer who sets up or moved offices to jurisdictions with no regulation or do not implement regulation governing virtual assets;

e) Customer who sets up new offices in jurisdictions with not clear business rationale underpinning the decision.

Price — 200,00 MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.