

This Document does not replace the need to consult the original version Published in official Gazette II. Series, no. 149, of 8 November, combined with Errata No. 5/21, of 17 December, published in the official Gazette I. Series no. 237.



COMISSÃO
DO MERCADO
DE CAPITAIS
REPÚBLICA DE ANGOLA

Regulation No. 5/2021

of 8 of November

On Prevention and Combating Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction

Whereas Law No. 5/20 of 27 January on the Prevention and Combating of Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction revoked Law No. 34/11 of 12 December on Combating Money Laundering and Terrorist Financing.

Whereas, furthermore, the aforementioned Law has reinforced, on the one hand, the obligations to which institutions subject to supervision by the Capital Market Commission (CMC) are bound, as well as reiterating the powers to supervise and monitor compliance with obligations of a preventive

and repressive nature to combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, and to regulate the rules on the creation of instruments, mechanisms and formalities inherent to effective compliance with the obligations set out therein, on the other hand.

Taking into account the duties of diligence, information and communication to which the entities subject to the supervision of CMC are obliged, by virtue of Law no. 1/12 of 12 January, on the Designation and Enforcement of International Legal Acts and Presidential Decree 214/13 of 13 December regulating it, it has proved necessary to revise Regulation 4/16 of 2 June laying down the conditions for the prevention of money laundering and terrorist financing.

Accordingly, under Article 57.2 (a) of Law No. 5/20 of 27 January on Preventing and Combating Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction, Article 33.1 of the Securities Code, combined with Article 4(1) and Article 19(c) of the Organic Statute of the CMC, approved by Presidential Decree No. 54/13 of 6 June, the Board of Directors of the Capital Market Commission hereby approves the following:

CHAPTER I

General Provisions

Article 1.

(Object)

1. This Regulation lays down the rules on the conditions for effective implementation of the obligations under Law No. 5/20 of 27 January on Preventing and Combating Money Laundering, Financing of Terrorism and Proliferation of Weapons of Mass Destruction (LPCBC-FT-PADM) and other related legislation.
2. This Regulation shall also establish the rules on the creation of instruments, mechanisms and formalities inherent to the obligations referred to in the preceding paragraph.

Article 2.

(Scope of application)

1. This Regulation shall apply to the following entities:
 - a) Non-banking financial institutions linked to the capital market and investment, subject to the supervision of the Capital Market Commission (CMC), under the terms of the Financial Institutions Act;
 - b) Banking financial institutions, regarding the activities developed by them within the scope of CMC's attributions, under the terms of Law on the General Regime of Financial Institutions;
 - c) Managing entities of regulated markets, settlement systems, clearing houses or central counterparties and centralised securities systems;
 - d) External auditors registered with the CMC, in everything that is not incompatible with their nature;
 - e) Securities investment advisers, duly authorised, in all matters not incompatible with their nature.
2. The present Regulation shall apply, with the necessary adaptations, to other entities that are subject to supervision by the CMC due to their nature and activity.
3. Without prejudice to their effectiveness, the entities referred to in paragraph 1(b) may establish measures of a preventive and repressive nature to combat money laundering, financing of terrorism and proliferation of weapons of mass destruction, with regard to the different sectors of activity in which they operate, which are common and assign duties to the same collaborators.

Article 3.

(Definitions)

Without prejudice to the definitions provided in Article 3 of the LPCBC-FT-PADM, for the purposes of these Regulations, the following definitions shall apply:

- a) *"Offshore Centres"* refer to corporate entities which are incorporated or bank accounts opened in a country other than the domicile of their owners, where they enjoy tax privileges, namely tax exemption or reduction of taxes;
- b) *"Client"* or *"Customer"* refers to any natural or legal person or any other legal entity with which the subject entities establish or have established a business relationship or carry out an occasional transaction;
- c) *"Collaborator"*, refers to any natural person who, on behalf or in the interest of the subject entities and under their authority or dependence, takes part in the performance of any operations, acts or procedures inherent to the activity pursued by the subject entity, irrespective of whether or not they have an employment link with the subject entity;
- d) *"Compliance Officer"*, is the person responsible for the compliance monitoring system on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;
- e) *"Front entity"*, a person acting in his own name in securities or derivatives transactions, whose ultimate purpose is to benefit a third person who has power and control over the transaction;
- f) *"Subject entities"*, those set out in Article 2;
- g) *"Suspicious operations"*, any and every act by a client that indicates or configures an attempt to conceal or disguise the nature, origin, location or ownership of assets, rights or values derived directly or indirectly from the commission of a crime, with a view to giving them a licit appearance;
- h) *"Representative"*, refers to the person legally representing the customer, as well as any agent, proxy, trustee, business manager or any other person entitled, alone or jointly with other representatives, to act in the name of and on behalf of the customer vis-à-vis the subject entities.

CHAPTER II
Obligations of the Subject Entities

Section I
Risk Assessment Obligation

Article 4.
(Risk assessment)

1. The subject entities ensure compliance with the risk assessment obligation under Article 9 of the LPCBC-FT-PADM, by developing and implementing tools or information system for the effective management of the risk of money laundering, terrorist financing and the proliferation of weapons of mass destruction in relation to both new and existing customers, so as to ensure effective identification and due diligence measures appropriate to the identified risk profile.
2. The risk assessment carried out under the terms of the preceding number shall be updated at intervals not exceeding 12 months.
3. The subject entities may decide that the evaluations referred to in the previous paragraph shall be carried out periodically up to 24 months, whenever the nature, dimension and complexity of the activity carried out by them so justify and the specific operating reality or business area or product in question presents a lower exposure to the risks of money laundering, financing of terrorism and proliferation of weapons of mass destruction, and the justification shall be reduced to writing and retained under the terms of Article 16 of the LPCBC-FT-PADM.
4. The subject entity shall ensure that the results of the risk assessments referred to in the preceding paragraphs are reflected and effectively implemented in the policies, procedures and internal risk management and mitigation controls set up in the institution, as appropriate.
5. Subject entities shall assess the category of risk associated with customers and assign the degree of risk, as provided in Article 21.
6. The tools or information system for effective risk management referred to in paragraph 1 shall include:

- a) Documentation on the risks inherent to the specific operating reality of the subject entity and the way in which it has identified and assessed them, as well as on the adequacy of the means and control procedures aimed at mitigating the risks identified and assessed on how the subject entities monitor the adequacy and effectiveness of these means;
 - b) Consideration of all relevant risk factors before determining the overall level of risk and the appropriate type and extent of mitigation measures to be applied;
 - c) Continuous updating of risk assessments of the institution under review;
 - d) Use of appropriate technical and technological mechanisms to provide information on risk assessments to CMC;
 - e) Demonstration of the adequacy of the procedures adopted, whenever requested by the competent supervisory or oversight authority.
7. Subject entities must also:
- a) Develop and implement the policies, procedures and internal controls approved by the respective management body, in order to manage and mitigate the risks identified by them or communicated to them by CMC;
 - b) Assess the effectiveness of such policies, procedures and internal controls and improve them where necessary;
 - c) Ensure that the implementation of the simplified or enhanced measures referred to in the previous paragraph takes into account the assessed risk and the guidelines of the supervisory and oversight authorities.

Article 5.

(Sources of information)

1. For the identification, evaluation and mitigation of the concrete risks of money laundering, financing of terrorism and proliferation of weapons of mass destruction, the subject entity must make use of reputable, credible and diversified sources of information as regards their origin and nature.

2. In order to comply with the provisions of the preceding paragraph, the subject entity may resort, among others, to the following sources:
 - a) Information, guidelines or alerts issued or disseminated by the CMC, related to the types and methods of identification of specific or emerging risks or to indicators of suspicion;
 - b) Information, guidance or alerts from the Financial Intelligence Unit (FIU) or from law enforcement authorities, relating to the typologies and methods of identification of specific or emerging risks or to indicators of suspicion;
 - c) Information, guidelines or alerts issued by the Government, relating to the prevention and combating of money laundering, financing of terrorism and proliferation of weapons of mass destruction;
 - d) Information resulting from the national risk assessment;
 - e) Lists issued by public bodies, namely of relevant functions of a political or public nature or of their respective holders, when they exist;
 - f) Internal analyses and documents of the subject entity, including information collected during identification and due diligence procedures, as well as internally developed and updated lists and databases;
 - g) Independent and credible information coming from civil society or international organisations, such as:
 - i)* Corruption indices or specific assessment reports on jurisdictions where the subject entity operates;
 - ii)* Other publicly available reports or documents on levels of corruption and income associated with the performance of political or public functions in a particular country or jurisdiction;
 - iii)* Mutual evaluation reports of the Financial Action Task Force (FATF) or its regional type bodies; and
 - iv)* Any other listings issued by relevant international organisations on the matter.
 - h) Information from the internet and media, provided it comes from a credible and independent source;

- i) The information contained in databases, lists, risk reports and other analyses from commercially available sources in the market;
 - j) Official statistical data of national or international source;
 - k) Relevant academic output; and
 - l) Information made available by other financial institutions or institutions of a similar nature, to the extent legally admissible.
3. The entity subject must adapt the use of the sources of information mentioned in the previous number to its specific operating reality, taking into account, at least, the risk factors identified under the terms of Article 9(1) and Article 10(1), both of the LPCBC-FT-PADM.

Article 6.

(IT tools and applications)

1. For the purposes of risk assessment, management and mitigation, the subject entity shall implement tools or computer applications that are instrumental or auxiliary to the fulfilment of the obligations and duties set out in the LPCBC-FT-PADM.
2. The tools and software applications referred to in the previous paragraph must enable, at least:
 - a) The registration of identifying data and other details of customers, their representatives and beneficial owners, as well as any updates thereof;
 - b) The detection of circumstances susceptible to parameterisation that should justify the updating of the identifying data and other elements relative to the customers referred to in the previous subparagraph;
 - c) The definition and updating of the risk profile associated with customers, business relationships, occasional transactions and operations in general;
 - d) The monitoring of customers and operations against identified risks, including the timely detection of:
 - i)* Relevant changes to the operating pattern of a given customer or set of related customers; and
 - ii)* Operations or set of operations that denote elements of suspicion.

- e) The detection of the acquisition of the quality of EPP or of holder of other political or public office, as well as of any other specific quality that should motivate the intervention of a member of top management or of another element of a higher hierarchical level;
 - f) The detection of any persons or entities identified as having restrictive measures, in particular those emanating from a United Nations Security Council resolution or otherwise;
 - g) The blocking or suspension of the establishment or continuation of a business relationship, as well as the carrying out of an occasional transaction or operation in general, whenever they depend on the intervention of a member of top management or of another element of a higher hierarchical level;
 - h) The blocking or suspension of the execution of operations or a set of operations, namely when:
 - i)* The subject entity should refrain from carrying out a given transaction or set of transactions in view of the existence of potential suspicions; and
 - ii)* The subject entity shall comply with the freezing obligations arising from financial penalties referred to in subagraph (f).
 - i) The timely extraction of reliable and comprehensible information to support analysis and decision-making by the relevant internal structures, as well as compliance with the legally established reporting and collaboration obligations.
3. The tools and information systems referred to in the previous paragraphs, in particular as regards their level of computerisation and parameterisation, must be proportional to the nature, size and complexity of the activity of the subject entity, as well as to the risks associated with each of the respective business areas, without prejudice to the provisions of the final part of paragraph 7.
4. Notwithstanding the provisions of the previous number, the subject entity must also adopt tools and applications that allow:
- a) Assessing the status of holder of another political or public office prior to establishing the business relationship or carrying out the occasional

- transaction, as well as the supervening acquisition of that status in the course of the business relationship; and
- b) To identify on an ongoing basis the degree of risk associated with business relationships and occasional transactions, as well as changes in that degree of risk in the course of the business relationship.
5. After the cessation of the exercise of any of the positions or the capacity referred to in subparagraph (a) of the preceding paragraph, the subject entity shall adopt procedures aimed at assessing whether its clients continue to represent an increased risk of money laundering, financing of terrorism and proliferation of weapons of mass destruction, in accordance with their profile and the nature of the operations developed before and after the said cessation.
 6. The subject entity ensures that the adoption of the IT tools and applications is made in order to guarantee their full and immediate access, whenever requested by CMC.
 7. Depending on the financial capacity, business volume, risk of the activity and mitigation capacity, proof of compliance with the obligations of preventing and combating money laundering, financing of terrorism and proliferation of weapons of mass destruction, the subject entity may request CMC to waive the implementation of computer applications referred to in Paragraph 1.

Section II

Duty of Identification, Diligence and Refusal

Subsection I

Obligation to Identify

Article 7.

(Obligation to identify customers)

1. The identification and due diligence obligations, provided for in Article 11 of the LPCBC-FT-PADM shall be adopted by the subject entities in

respect of their clients and, if applicable, their representatives and beneficial owners.

2. The identification and due diligence obligations apply not only to new customers, but also to existing customers, depending on the assessment of the risk of money laundering, financing of terrorism and proliferation of weapons of mass destruction associated with them.
3. Whenever the subject entities become aware or have reasonable suspicion that the customer is not acting on their own account, they should take appropriate measures to enable them to know the identity of the person or entity on whose behalf the customer is acting, namely the beneficial owners.
4. To identify the beneficial owners, the reporting entities shall verify the existence of a mandate, fiduciary or controlling relationship or any other type of significant influence, regardless of its nature.
5. In the event of doubt as to the true identity of the customer and, where applicable, the representative or beneficial owner, which cannot be resolved satisfactorily, reporting entities shall refuse to enter into any transactions or shall terminate such transactions if necessary.

Article 8.

(Establishing the business relationship)

1. For the purposes of identification and verification of identity, pursuant to the provisions of Article 11(2) of the LPCBC-FT-PADM, the subject entities shall collect and retain information on the customers, their representatives and beneficial owners, if applicable, before the start of the business relationship, and shall request at least the following elements:
 - a) Physical persons:
 - i)* Full name and signature;
 - ii)* Date and place of birth
 - iii)* Nationality;

- iv)* Complete and updated address of domicile or any other contacts, considered as valid by the respective subject entity or the certificate of residence;
 - v)* Profession and employer, if any;
 - vi)* Nature and amount of income;
 - vii)* Name and number of identification document used, date of issue, date of expiry and issuing body;
 - viii)* Taxpayer Number (VAT Number);
 - ix)* Public or political positions held or duties;
 - x)* Duly signed power of attorney granting powers of representation, if applicable.
- b) Legal persons:
- i)* Full company name;
 - ii)* Object and purpose of the business;
 - iii)* Head Office Address;
 - iv)* VAT Number;
 - v)* Commercial Registry Number;
 - vi)* Indication of the holders of shareholdings in the share capital or in the voting rights of the legal person of a value equal to or greater than 20%, with an indication of the percentage of each, as well as:
 - i.* Indication of the existence of shareholders' agreements or any type of concerted action agreement between shareholders and, if so, a copy of the agreement;
 - ii.* Identification of shareholdings held indirectly in the company through a company in a controlling or group relationship, through a fiduciary business or through an agreement for the management of shareholdings or for the exercise of voting rights.
 - vii)* Indication of the representatives of the legal person and their mandate.
- c) Sole Traders, in the establishment of the business relationship:
- i)* Original document or photocopy of the certificate of the public deed of incorporation or equivalent document, commercial registry

certificate, publication in the Official Gazette, permits or any other valid licence issued by the competent authority;

- ii)* Full company name;
 - iii)* Headquarters and activities;
 - iv)* VAT Number;
 - v)* Identification details referred to in point (a) of this paragraph, where applicable.
- d) In relation to condominiums of immovable property under the regime of horizontal property and separate property, constituted under the terms of the legislation in general or legal interest centres without legal personality, the regime set out in paragraph (b) shall apply, with the necessary adaptations.
2. The verification of the information must be proven by the presentation of the following valid documents:
- a) Physical persons:
 - i)* The identification elements mentioned in points i), ii), iii) and ix) of paragraph 1(a) shall be verified as follows:
 - i.* Exchange residents, on presentation of a valid Identity Card or Resident Card issued by the competent authority, containing a photograph, full name, signature, address, date of birth and nationality;
 - ii.* For non-exchange residents, upon presentation of a valid passport, except for non-exchange residents of Angolan nationality, upon presentation of a valid Identity Card;
 - iii.* The complete address, profession, the respective employer, if any, through the work declaration or residence certificate or any other valid document, suitable and sufficient to check the truthfulness of the information provided;
 - iv.* The identification element mentioned in point *ix)* of paragraph a) of no. 1, through a declaration issued by the person himself/herself with the list of the positions of public or political nature held.
 - b) Legal persons:

- i)* For resident legal persons, the identification elements mentioned in paragraphs i), ii), iv) and v) of sub-paragraph b) of no. 1 shall be verified by the presentation of the Certificate of Commercial Registry issued by the Commercial Registry Office or other public documentary proof, namely the copy of the Official Gazette containing the publication of the Articles of Association or the notarial certificate of the deed of incorporation, or the address of the website, maintained by the relevant Ministerial Department, where the identification elements above mentioned have been published;
- ii)* In relation to non-resident legal persons, the identification elements mentioned in points i), ii) and v) of paragraph b) of no. 1, shall be verified through the presentation of proof of the commercial register or other valid public document, duly certified by the competent entities of the country of residence and authenticated by the Angolan consular representation that has jurisdiction over the territory where the document was issued;
- iii)* The identification element mentioned in point iv) of paragraph 1(b) shall be verified by the presentation of the VAT number;
- iv)* The identification element mentioned in point v) of paragraph 1(b) shall be verified by means of:
 - i.* Certificate of the Commercial Registry and of the communications made under the terms of paragraph 4 of Article 251 of Law No. 1/04 of 13 February, of Commercial Companies, in the case of private limited companies;
 - ii.* Declaration of the issuer, in the case of public limited companies with registered shares;
 - iii.* Declaration of the issuer, in the case of public limited companies with registered shares;
 - iv.* Copy of the attendance list of the last five General Meetings or the certified copy of the registration request with the depositary with the signature of receipt, when the securities are

- already deposited, in the case of public companies with bearer shares;
- v. Copy of the communications made under the terms of paragraph 1 of Article 466 of Law No. 1/04 of 13 February, of Commercial Companies, in the case of private limited companies, in any other case;
 - v) The identification element mentioned in point vi) of paragraph b) of no. 1 shall be proved by a written declaration issued by the legal person itself, containing the names of the holders of the management body, proxies or legal representative.
- c) When establishing the business relationship on behalf of minors who, due to their age, do not hold any of the documents referred to in subparagraph a) of the present number, the identification elements of the minor shall be verified:
- i) In case of foreign residents, by showing their personal identity card, when under six years old, and Identity Card, when over six years of age;
 - ii) In the case of a non-resident foreign exchange resident, by an equivalent public document, to be presented by the person who demonstrates legitimacy as his/her legal representative for the establishment of the business relation.

Article 9.

(Momento of identification check)

1. The subject entities shall identify the customers and, if applicable, the representatives and beneficial owners, and take reasonable measures to verify their identity, at the time when the business relationship is established or before any occasional transaction takes place.
2. Unless otherwise provided by law or regulation, subject entities may complete the identification and verification procedures, after the establishment of the business relationship, provided that:
 - a) The risk of money laundering, terrorist financing and the proliferation of weapons of mass destruction is reduced;

- b) The procedures take place within a maximum period of 15 days, counting from the beginning of the business relationship;
 - c) It is essential in order to not interrupt the normal course of business, namely in the following circumstances:
 - i) They are transactions carried out without the physical presence of the customer;
 - ii) They are transactions corresponding to the exercise of corporate rights over securities.
 - d) They adopt a system to prevent and combat money laundering, terrorist financing and the proliferation of weapons of mass destruction that includes the conditions under which untimely verification may occur, *inter alia*:
 - i) Limiting the number, type or value of transactions to be carried out at a time before identity verification;
 - ii) Reinforced monitoring of the business relationship between the time of its establishment and identity verification.
 - e) Paragraph 2(a) shall not apply, even if the risk is low, where there is a suspicion that the transaction is related to the crime of money laundering, financing of terrorism and proliferation of weapons of mass destruction or other crimes underlying them, in which case paragraph 1 shall apply.
3. If the subject entities are unable to obtain the required information about the customer in a timely manner, they shall refrain from establishing the business relationship or carrying out any occasional transaction.

Article 10.

(Occasional transactions)

1. The subject entities shall collect and maintain the information whenever, in person or remotely, a customer intends to perform occasional transactions, in the amount to be indicated by CMC by Instruction, regardless of whether the transaction is performed through a single operation or through several operations that appear to be related.

2. As a minimum, pursuant to Article 8(1) and (2), identification details and corresponding supporting documents of the person or entity intending to carry out the transaction and, if applicable, of their representatives and beneficial owners shall be required, as follows:
 - a) Natural persons: elements provided for in points *i), ii), iii)* and *vi)* of Article 8.1(a);
 - b) Legal persons: elements provided for in points *i), ii), iii)* and *vi)* of Article 8.1(b);
 - c) Sole Traders: elements provided for in Article 8(1)(c);
 - d) Condominiums of immovable horizontal property and independent properties: elements provided for in Article 8(1)(d).
3. Where occasional transactions are required to be carried out on behalf of minors who, on account of their age, do not hold any of the documents referred to in subparagraph (a) of paragraph 2 of Article 8, the identification details of the minor shall be verified in accordance with sub-paragraph (c) of paragraph 2 of Article 8.
4. In cases where the number of operations carried out by a customer shows a pattern of frequency, institutions should consider this to be a stable and long-lasting relationship, qualifying it, from then on, as an effective business relationship and adopting the corresponding identification and due diligence procedures.

Article 11.

(Mechanisms to identify the beneficial owner)

In addition to the elements mentioned in paragraph 1(a) and the evidence mentioned in paragraph 2(a), all of Article 8, identification of the beneficial owner should include a copy of the trust or partnership agreement, if any, a certified copy of the document confirming its identification or the latest minutes of the constitutive General Assembly, or other equivalent document, in case the transactions or operations are carried out on behalf of the beneficial owner and not of the customer.

Article 12.

(Identification of collaborators)

The employees of the subject entity who carry out the identification and due diligence obligations, namely the collection, recording and verification of the evidence submitted, shall mention in the internal supporting records their identification and the date on which they performed those acts.

Subsection II

Duty of Diligence and Refusal

Article 13.

(Duty of continuous monitoring)

1. As part of the obligations under Article 11(2)(f) of the LPCBC-FT-PADM, for the purposes of ongoing monitoring of the business relationship, depending on the customer's risk assessment, the following information should be requested in relation to the customer:
 - a) Nature, purpose and details of the business;
 - b) Registration of house moving;
 - c) Professional data;
 - d) Origin of assets to be used in the business relationship;
 - e) Origin of initial and ongoing income;
 - f) The various relationships between customers and their beneficial owners, if applicable.
2. Subject entities, whenever they deem necessary, should request additional information from clients, in view of the transactions carried out by them and the risk assessment carried out, such as the annual report and accounts, among others.
3. The management bodies of the subject entities should be aware of the profile of the high-risk customers of the institution they manage.

Article 14.

(Enforcement of obligations by third parties)

1. For the purposes of Article 26(1) of the LPCBC-FT-PADM, the subject entities provided for in paragraphs a) and b) of Article 2(1) may only use other subject entities of a financial nature, registered with the CMC or other group entities domiciled in a third country that meet the requirements set out in Articles 11 to 14 of that Law.
2. The enforcement of obligations by third parties does not apply to contracts for the subcontracting of services, also known as *outsourcing*, or to contracts with correspondents.

Article 15.

(Qualification requirements for the third party entity)

1. For the purposes of the previous article and the provisions of Article 26(2) of the LPCBC-FT-PADM, financial institutions shall only consider that a third party entity is qualified to perform identification and due diligence procedures on their behalf if the following cumulative requirements are met:
 - a) The third party entity has a system of internal control for the compliance monitoring system on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;
 - b) The third-party entity has all the means necessary to perform the identification and due diligence procedures on behalf of the subject entity, as well as human resources with the necessary qualification and training for that purpose;
 - c) The third party entity ensures that the procedures are carried out with the necessary speed, that adequate records of the information collected are kept and that the information is immediately and permanently available to the subject entity.
2. Without prejudice to the possibility of deferred verification of the identification and due diligence procedure, financial institutions shall

obtain from the third party entity all data and elements legally required prior to establishing a business relationship or carrying out an occasional transaction, also ensuring:

- a) Reducing to writing the measures taken to ensure that the third party entity is regulated and supervised with respect to the prevention and combating of money laundering, terrorist financing and the proliferation of weapons of mass destruction;
- b) The writing down of the results of the inspection carried out to the third party entity regarding the implemented measures to, effectively, comply with the obligations set out in Articles 11 to 14 of the LPCBC-FT-PADM.

Article 16.

(Information previously collected by a third party entity)

1. The financial institutions establishing business relations or carrying out occasional transactions on behalf of customers whose identification and due diligence details as well as beneficial ownership information have previously been collected by another financial subject entity within the same economic relationship may rely on the customer information transmitted to them by that other subject entity.
2. In the case set out in the preceding paragraph, the financial institution that uses a third party entity to collect the identification and due diligence elements and the information on the beneficial owner of its customers shall ensure:
 - a) That the third party entity's procedures are adequate, in particular whether it has procedures in place for the identification and due diligence, as well as for the monitoring of risk situations for the prevention and combating of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction;
 - b) The implementation of adequate procedures and information flows to allow for the fulfilment of the duties to which it is bound under the terms of the LPCBC-FT-PADM and the present Regulation, including the adoption of increased due diligence measures.

Article 17.

(Correspondents)

1. In those cases in which, in accordance with the applicable legal system, it is permissible for subject entities to carry out their activities through correspondents, they shall ensure that correspondents carry out the customer identification and due diligence measures established in Articles 11 to 14 of the LPCBC-FT-PADM.
2. The correspondents shall make available, whenever requested by the subject entities, the documentation obtained during the implementation of the measures foreseen in the previous number, as well as any other documentation deemed relevant.
3. Without prejudice to the provisions of the preceding paragraph, the subject entities shall ensure compliance with the correspondents' legal and regulatory obligations.
4. When establishing a business relationship or occasional transaction, through a correspondent, the above entities shall, as a minimum, ensure the following measures:
 - a) Set up internal control and periodic risk assessment mechanisms to ensure the effective control of the correspondents' activity and the prevention and fight against money laundering, terrorist financing and the proliferation of weapons of mass destruction.
 - b) Monitor the transactions carried out through the correspondent;
 - c) Assess, on a regular basis, the effectiveness of the policies, procedures and internal controls to prevent and combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction implemented by correspondents.
5. Subject entities shall keep an updated list of all their correspondents, which shall be made available to CMC whenever requested.

Article 18.

(Simplified due diligence procedures)

1. Subject entities, in their internal policies, procedures and controls referred to in Article 9(5)(a) of the LPCBC-FT-PADM, shall:
 - a) Establish, on the basis of the specific risk of money laundering, terrorist financing and proliferation of weapons of mass destruction, the criteria for classifying customers as eligible for simplified measures;
 - b) Establish the set of simplified measures that will apply to customers classified under the terms of the previous subparagraph, defining, namely, the frequency and intensity of monitoring and updating procedures;
 - c) Establish procedures for the surveillance and monitoring of customers to enable the possible update of the classification referred to in paragraph (a) and the adjustment of the measures applied under paragraph (b).
2. The subject entities shall include in the documentation to be kept under the terms of Article 16 of the LPCBC-FT-PADM, where applicable, information on the adoption of simplified measures and the period of their implementation
3. For the purposes of Article 13(4) of the LPCBC-FT-PADM, in the risk analysis, subject entities shall also consider the following factors:
 - a) Nature of the client, namely whether it is a natural person or a legal person with a simple and transparent control structure;
 - b) Clearly identified beneficial owners domiciled in national territory or in geographical locations referred to in Article 23(1)(c);
 - c) Professional activities or economic activities developed by the client without complexity and with low turnover;
 - d) Regularity in the amounts and type of customer transactions;
 - e) Other relevant factors indicating a low risk of money laundering, terrorist financing and proliferation of weapons of mass destruction.

Article 19.

(Enhanced due diligence procedures)

1. The subject entities shall define and adopt the enhanced due diligence measures referred to in Article 14 of the LPCBC-FT-PADM in a manner that is proportionate and appropriate to the degree of risk associated with the customer, the beneficial owner or the transaction, taking into account the specific circumstances of the business relationship or occasional transaction.
2. For the purposes of the preceding paragraph, increased due diligence measures are considered to be, among others:
 - a) Obtaining additional information on customers, their representatives or beneficial owners, and on transactions;
 - b) The performance of additional diligence to corroborate the information obtained;
 - c) The intervention of a member of the senior management or another element of a higher hierarchical level is required for the authorisation of the establishment of business relations, the execution of occasional transactions or the conduct of operations in general;
 - d) The strengthening of procedures for monitoring operations in order to detect possible indicators of suspicion and, if these are found, the subsequent communication to the FIU;
 - e) The intensification and application of complementary measures for monitoring operations carried out without the physical presence of the customer, its representative or the beneficial owner, and confirmation of identity may be supplemented with additional documents or information provided by the customer and considered sufficient for the purposes of confirmation or verification;
 - f) Reducing the time intervals for updating the information received relating to the identification details of customers, representatives and beneficial owners, other items of information provided for in this Regulation and the means of providing evidence of those details;
 - g) Permanent monitoring of the business relationship by the *Compliance Officer* or another employee of the subject entity who is not directly

- involved in the business relationship with the customer or other persons especially related to the customer;
- h) Obtaining information on the origin and destinations of assets
3. The subject entities shall put in writing the result of the measures referred to in the preceding paragraph and keep available the record of the operations in which they use the enhanced due diligence measures for consultation by the CMC.
 4. CMC shall establish by Instruction the procedure for verification of the origin and destination of the assets, for the purpose of paragraph 2(h).
 5. Without prejudice to the adoption of the specific procedures provided for in the other articles related to the section on identification, due diligence and refusal obligation of the above-mentioned Regulation, special consideration shall be given to the adoption of enhanced due diligence measures, appropriate to the concrete risks identified, with regard to situations indicating potentially higher risk, identified in Article 23.
 6. For the purposes of compliance with the assumptions set forth in paragraph 2(g), the subject entities shall comply with the information conservation requirements set forth in Article 16 of the LPCBC-FT-PADM.

Article 20.

(Politically exposed persons)

1. Without prejudice to the identification and due diligence duties provided for in the previous sections of this Chapter, subject entities shall ensure, when applying enhanced due diligence measures in relation to transactions carried out with PPE, pursuant to Article 14(5) of the LPCBC-FT-PADM, that:
 - a) The information on the identification processes and procedures relating to PPE is communicated to those of its collaborators for whom it is relevant;
 - b) The enhanced due diligence measures, referred to in Article 14(5) of the CPLP-FT-PADM, shall be part of its training programme for preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;

- c) The enhanced due diligence measures are appropriate and tailored to each individual case, taking into account a risk-based assessment of the services or products purchased, individual circumstances and the origin and amount of the client's assets;
 - d) There is strict and permanent monitoring in its relationship with the PPEs, with regard to the transfer of assets.
2. Without prejudice to the measures established in the previous number, the CMC establishes by means of a Ruling, the minimum content of operational procedures for implementing the obligation of applying increased due diligence measures in the business relationship or occasional transactions and operations with PPEs.

Article 21.

(Transactions carried out without the physical presence of the customer)

1. For the purposes of Article 14(4) of the LPCBC-FT-PADM, subject entities, in transactions carried out without the physical presence of the customer, shall:
- a) Apply the identification and due diligence procedures provided for in the previous sections;
 - b) Include continuous monitoring in the establishment and during the business relationship or when conducting occasional transactions, as with customers who are physically present.
2. Subject entities, as part of the specific and appropriate measures to mitigate the risks inherent in operations carried out without the physical presence of the customer, should, as the case may be:
- a) Require that the documents requested under Article 8(2)(a) are recognised or certified by a competent authority;
 - b) Request additional documents to supplement those indispensable for customers physically present, requested under Article 8(2).

Article 22.

(Non-profit organisations)

1. In addition to the identification and due diligence duties provided for in the previous sections and in accordance with Article 14(1) of the LPCBC-FT-PADM, subject entities should establish appropriate enhanced due diligence procedures for transactions with non-profit organisations, in the framework of preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.
2. The procedures referred to in the previous paragraph shall include the collection and recording of the following information:
 - a) Statutes and organisational structure;
 - b) Documentary proof of legalisation by a public authority;
 - c) Nature and purpose of the organisation's activities;
 - d) Names of all managers or equivalent;
 - e) Names or classes of beneficiaries;
 - f) Geographical location;
 - g) Origin of donations and volunteering;
 - h) Source of assets and expenses, including beneficial ownership information.

Article 23.

(Risk factors justifying enhanced due diligence)

1. The following indicators, among others, are considered as high risk factors that may trigger enhanced due diligence:
 - a) Factors related to clients and beneficial owners:
 - i)* Legal persons or arrangements which are vehicles for holding personal assets;
 - ii)* Companies with fiduciary shareholders or having their share capital represented by bearer shares;
 - iii)* Ownership or control structures that appear unusual or excessively complex given the nature of the activity pursued by the customer/beneficiary;

- iv)* Actual customers/beneficiaries resident or operating in the States that represent a risk factor due to their geographical location;
- v)* Actual clients/beneficiaries who have been subject to sanctions or restrictive measures imposed by the United Nations Security Council or by the Angolan State;
- vi)* Customers who are in one of the following circumstances:
 - i.* Who show reluctance or refuse to provide the identification elements, supporting evidence and other information or verification requested;
 - ii.* Who provide information that is not very credible as to its authenticity, not very explicit as to its content, difficult to verify by the entities subjected to it or with unusual characteristics;
 - iii.* Who repeatedly provide documents or information other than those requested.
- vii)* Clients who show reluctance or refuse to establish face-to-face contact with the subject entity or who do not wish correspondence to be sent to the declared address;
- viii)* Clients who, with no apparent relation between them, have common contact details, or who present details that prove to be incorrect or are permanently inoperative, or change frequently;
- ix)* Clients who only seek to establish contact with a specific employee or employees of the same subject entity, in particular when, in view of the absence of such employee or employees, they decide not to execute or to suspend operations;
- x)* Clients showing unusual concern about the confidentiality of transactions processed through the subject entity;
- xi)* Clients showing an unusual and unreasonable knowledge of the legislation preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction or showing an unusual interest in knowing the policies, procedures and internal controls of the subject entity aimed at preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;

- xii)* Clients related to operations suspected of money laundering, financing terrorism and the proliferation of weapons of mass destruction, market manipulation or insider trading;
 - xiii)* Clients with no discernible connection to use the services of the subject entities.
- b) Factors related to operations and services:
- i)* Transactions involving cash transactions intensively and without plausible explanation;
 - ii)* Transactions with repeated capital gains and losses;
 - iii)* Movements outside the scope of investment accounts and sudden stopping of transactions in thinly traded, large accounts;
 - iv)* Transactions at off-market prices;
 - v)* Transactions involving the acquisition of assets of significant value and which, in a short period of time and for no apparent reason, proceed to their sale or depreciation;
 - vi)* Transactions in securities with a low market price;
 - vii)* Transactions involving securities in pooled accounts;
 - viii)* Opening accounts or purchasing products or services of material importance without any concern for potential losses, commissions or other costs associated with those products and services;
 - ix)* Transactions in derivative financial instruments or other circumstances that are unusual, in view of the customer's expected profile and other elements characterising the business relationship or occasional transaction, in particular when customers provide unclear or inconsistent explanations of transactions or have little knowledge of the purpose of the transaction, or when the customer expresses nervousness or unusual urgency in carrying out the transaction;
 - x)* Transfers of securities or financial instruments without consideration;
 - xi)* Change in account holders;
 - xii)* Re-specification of principals, namely in accounts with identical legal representatives;

- xiii)* Intensive transactions on bearer securities or others that allow the anonymity of the respective holder;
- xiv)* Transactions that show a degree of complexity that is apparently unnecessary for the achievement of the purpose for which they are intended;
- xv)* Transactions whose purpose or economic rationality is not evident;
- xvi)* Transactions that have no connection with the known activity of the client and which involve persons or entities related to States publicly recognised as locations for the production or trafficking of narcotics, with high levels of corruption, money laundering platforms, promoters or supporters of terrorism, promoters or supporters of the proliferation of weapons of mass destruction or other States with highly restrictive legislation on banking secrecy;
- xvii)* Early cessation of a product, especially involving loss;
- xviii)* High turnover of intermediaries or financial consultants;
- xix)* Transactions on behalf of minors or disabled persons, without justification;
- xx)* Transactions with subject entities through a non-resident foreign exchange correspondent in cases where the sole purpose is to carry out portfolio investment;
- xxi)* Fractionation of transactions or transactions below the legal limit for compliance with registration or reporting obligations with a view to preventing and combating money laundering, financing of terrorism and proliferation of weapons of mass destruction;
- xxii)* Unusual intermediation, such as the payment of unusually high compensations or commissions;
- xxiii)* Transactions that are unusual for the client's profile, incompatible with the time zone or sudden change in the usual nature of transactions;
- xxiv)* Pattern of transactions with significant losses;
- xxv)* Application for the discounting of bearer securities without deposit in an account;
- xxvi)* Systematic recourse to several jurisdictions;

- xxvii)* Reluctance to provide the requested identification elements, or complementary information, such as corporate structure, business purpose, business background or head office;
 - xxviii)* Request to forward payments to intermediaries' accounts;
 - xxix)* Transfer of assets across multiple accounts;
 - xxx)* Transfers between different customer-owned accounts with no apparent purpose or business;
 - xxxi)* Use of the securities account as a mere account of transfers or outflows of assets and reduced securities activity;
 - xxxii)* Use of national accounts by a foreign-based client to trade in foreign markets;
 - xxxiii)* Use of forged documents;
 - xxxiv)* Use of a front entity to carry out the acquisition of the securities;
 - xxxv)* Use of a payment services company to transfer assets;
 - xxxvi)* Use of several unlinked accounts;
 - xxxvii)* Use of newly created legal persons if the amount is large in comparison with their capital or activity;
 - xxxviii)* Any other operations which, due to their characteristics, in terms of the parties involved, complexity, amounts involved, means of execution, instruments used or the lack of economic or legal grounds, may constitute cases of money laundering, financing of terrorism and proliferation of weapons of mass destruction or related crimes.
- c) Factors related to geographical location:
- i)* States with strategic deficiencies in the field of preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, identified by the GAFI in a document published by that body;
 - ii)* Other States identified by credible sources as lacking effective systems to prevent and combat money laundering, terrorist financing and the proliferation of weapons of mass destruction;
 - iii)* States identified by credible sources as having a significant level of corruption or other categories of crimes underlying money

- laundering, financing of terrorism and proliferation of weapons of mass destruction;
- iv)* States that have been subject to additional counter-measures decided by the Angolan State;
 - v)* States subject to sanctions, embargoes or other restrictive measures imposed by the United Nations Security Council;
 - vi)* States providing funding or support for terrorist activities or for proliferation of weapons of mass destruction, or in whose territory known terrorist organisations operate, or in which proliferation of weapons of mass destruction occurs;
 - vii)* Offshore centres.
2. The CMC establishes, by Ruling, the additional risk factors that justify reinforced due diligence.

Article 24.

(Obligation of refusal)

1. In the situations set out in Article 15(1) and (2) of the LPCBC-FT-PADM the subject entity, as soon as the decision to terminate the business relationship has been made:
 - a) It inhibits any movement of assets associated with the business relationship, including through any means of distance communication;
 - b) It contacts the customer, within a maximum period of 30 days, so that the customer indicates the account to which the assets are to be returned, or appears in person before the subject entity to effect the return as defined by the subject entity; and
 - c) It preserves the assets, keeping them unavailable until their restitution is possible.
2. If the customer, in contact with the subject entity, delivers the elements whose lack determined the decision to terminate the business relationship and, in the absence of any suspicion, the subject entity may proceed to re-establish that relationship, carrying out all the identification and diligence procedures legally foreseen.

Section III
Obligation of Control

Article 25.

(Responsibility of the management body)

1. The management body of the subject entity is responsible for implementing policies, procedures and internal controls on preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.
2. The nature and extent of policies, procedures and internal controls should be adapted to the nature and risk associated with the business, as well as the size and complexity of the institution.
3. For the purposes of paragraph 1, the management body shall in particular:
 - a) Approve the policies, procedures and internal controls commensurate with the identified risk, in accordance with Article 4;
 - b) Have appropriate knowledge of the money laundering, terrorist financing and weapons of mass destruction risks to which the subject entity is exposed at all times, as well as of the processes used to identify, assess, monitor and control those risks;
 - c) Ensure that the organisational structure of the subject entity allows, at all times, the adequate enforcement of policies, procedures and internal controls, preventing conflicts of interest and, whenever necessary, promoting the separation of functions within the organisation;
 - d) Promoting a culture within the organisation to prevent and combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, encompassing all employees of the entity whose functions are relevant in this context, underpinned by high standards of ethics and integrity and, whenever necessary, the definition and approval of appropriate codes of conduct;
 - e) To appoint the Compliance Officer, as referred to in Article 22(1)(a) of the LPCBC-FT-PADM;

- f) Monitor the activity of the other members of top management, to the extent that they oversee business areas that are or may be exposed to risks of money laundering, financing of terrorism and proliferation of weapons of mass destruction;
 - g) To periodically monitor the effectiveness of the policies, procedures and internal controls referred to in paragraph 1, ensuring the implementation of appropriate measures to correct any deficiencies detected in them.
4. The governing body must ensure that the Compliance Officer:
- a) Exercises their duties in an independent, permanent and effective manner and with the decision-making autonomy required for such exercise;
 - b) They possess the suitability, professional qualifications and availability adequate for the exercise of the duties, and the results of this evaluation are made available to CMC, whenever requested;
 - c) They have adequate technical, material and human resources and means, including the employees necessary for the good performance of the duties;
 - d) They have full and timely access to all internal information relevant to the exercise of their duties, in particular that relating to the execution of the duty of identification and due diligence and to the records of the operations carried out; and
 - e) They are not subject to potential functional conflicts, especially when there is no segregation of duties.
5. The management body shall refrain from any interference in the fulfilment of the duty to report provided for in Article 17 of the LPCBC-FT-PADM, whenever it is concluded that potential suspicions exist.
6. The designation referred in paragraph 3(e) shall be subject to previous registration with the CMC, under the rules of registration of the responsible persons with relevant management duty.
7. For the purposes of paragraph 4(d), relevant information means:
- a) Financial information of the customer, the beneficial owner or any person acting on behalf of a third party;

- b) Characteristics of the transaction;
- c) Records of past transactions, transaction patterns and volume or information regarding other products or services provided to the same customer;
- d) Duration of the business relationship;
- e) Communications previously made to the FIU regarding the same customer.

Article 26.

(Compliance officer)

1. The subject entities must designate a Compliance Officer for preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction, responsible for the following:
 - a) To coordinate and monitor the effective implementation and respective compliance with the appropriate policies, procedures and internal controls defined within the framework of the system for preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction;
 - b) Participate in the definition of and give prior opinion on policies, procedures and internal controls aimed at preventing money laundering, the financing of terrorism and the proliferation of weapons of mass destruction;
 - c) Continuously monitor the adequacy, sufficiency and timeliness of policies, procedures and internal controls for the prevention of money laundering, terrorist financing and the proliferation of weapons of mass destruction, and propose any necessary updates;
 - d) To participate in the definition, monitoring and evaluation of the subject entity's internal training policy;
 - e) Ensure the centralisation of all relevant information coming from the various business areas of the subject entity;
 - f) To communicate, without internal or external interference, the operations mentioned in Article 17 of the LPCBC-FT-PADM to the FIU;

- g) To play the role of interlocutor with the law enforcement, supervisory and oversight authorities, namely by complying with the reporting obligation provided for in Article 17 of the LPCBC-FT-PADM and ensuring compliance with the other reporting and collaboration obligations;
 - h) To support the preparation and implementation of the assessment provided for in Article 9 of the LPCBC-FT-PADM and the assessment of the effectiveness of the internal control system; and
 - i) Coordinate the preparation of reports and other information to be sent to the CMC on preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction.
2. Subject entities may also appoint a Compliance Officer who is not a member of their staff, provided that the designated person also performs this function in a subject entity of the same group subject to the supervision of the CMC, the National Bank of Angola or the Angolan Agency of Supervision and Regulation of Insurance, or is an auditor registered with the CMC.
 3. The subject entity ensures that all its collaborators, regardless of the nature of their employment relationship, are aware of:
 - a) The identity and contact details of the designated Compliance Officer, pursuant to Article 25(3)(e); and;
 - b) The procedures for reporting suspicious conduct, activities or operations detected by the Compliance Officer.
 4. The subject entity also ensures that the selection of the staff allocated to the compliance area or function is made based on high ethical standards and demanding technical requirements.
 5. Subject entities under Article 2(1)(a) and (e) may, depending on their financial capacity, business volume and identified risk, request CMC to waive the requirement of appointing an exclusive Compliance Officer, whereby, however, the duties provided for in paragraph 1 shall be performed by a designated employee, taking into account the provisions of Article 25(4)(b).

6. Without prejudice to the exclusive exercise by the employee appointed under the terms of the preceding paragraph of all powers legally attributed to them, subject entities may appoint a member of their management body to monitor matters related to the prevention and combating of money laundering, financing of terrorism and proliferation of weapons of mass destruction.
7. In the case foreseen in the previous paragraph, the subject entities shall communicate to CMC, the identity and direct contacts of the member of its designated management body, within five days of the designation.

Article 27.

(Assessment of the effectiveness of the internal control system)

1. The entities subject to the proceedings shall ensure that assessments of the internal control system are carried out, pursuant to Article 22(1)(c) of the LPCBC-FT-PADM, with the frequency referred to in Article 4(2)
2. The entities subject to the service may stipulate that the assessments referred to in the previous number shall be carried out with the frequency and under the terms laid down in Article 4(3);
3. The assessments referred to in paragraph 1 shall be proportionate in scope to the nature, size and complexity of the subject entity, as well as to the risks associated with each of its business areas, and:
 - a) Have unrestricted and timely access to all internal information relevant to the conduct of the assessments, including any documents prepared in compliance with the Law or the present Regulation;
 - b) To be assured in an independent manner by the internal audit function, by external auditors or by a duly qualified third party entity that guarantees the independence of that evaluation;
 - c) To be carried out with a frequency appropriate to the risk associated with each of the business areas of the entities subject to the audit;
 - d) Allow the detection of any deficiencies affecting the quality, adequacy and effectiveness of the adopted policies, procedures and internal controls; and
 - e) They concern, at least, the following:

- i)* The risk management model of the subject entity and other policies, procedures and internal controls designed to comply with the provisions of this Chapter;
 - ii)* The quality of the communications and other information provided to the CMC;
 - iii)* The status of implementation of corrective measures previously adopted;
 - iv)* The identification and due diligence and conservation procedures adopted, including those carried out by third parties;
 - v)* The integrity, timeliness and comprehensibility of the reports and reports generated by the information tools or systems, provided for in Article 9(2) of the LPCBC-FT-PADM;
 - vi)* The adequacy of customer and transaction monitoring procedures and controls, whether automated, manual or mixed;
 - vii)* The adequacy, comprehensiveness and timeliness of the processes for examining and reporting suspicious transactions;
 - viii)* The internal training policy of the subject entity, including the adequacy and scope of the training provided; e,
 - ix)* The promptness and sufficiency of corrective procedures for deficiencies previously detected in audit or oversight actions related to the prevention and combating of money laundering, terrorist financing and the proliferation of weapons of mass destruction.
4. Whenever the subject entity detects any deficiencies under the provisions of paragraph (d) of the preceding subsection, they should strengthen the policies, procedures and internal controls adopted to prevent and combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction by taking the necessary corrective measures to remedy shortcomings.
5. The results of the assessments referred to in paragraphs 1 and 7 shall be put in writing and kept under the terms of Article 16 of the LPCBC-FT-PADM and made permanently available to the CMC.

6. Subject entities where the existence or outsourcing of an internal or external audit function or a suitably qualified third party is not feasible or appropriate in view of the nature, size and complexity of the activity pursued are exempted from compliance with paragraph 3(b).
7. The subject entities referred to in the previous number shall ensure that effectiveness evaluations are carried out by an internal structure unit or a duly qualified employee with the frequency laid down in Article 4(2) and (3) and under the terms set out in the previous numbers.

Article 28.

(Receipt of irregularity reports)

1. The subject entities shall establish specific, independent and confidential channels that internally ensure, in an appropriate manner, the receipt, treatment and filing of reports of irregularities related to possible breaches of the LPCBC-FT-PADM, of this Regulation and the policies, procedures and internal controls established to prevent and combat money laundering, terrorist financing and the proliferation of weapons of mass destruction.
2. The channels referred to in the previous paragraph must:
 - a) Be proportionate to the nature, size and complexity of the business of the subject entity; and
 - b) Ensure the confidentiality of communications and the protection of personal data of the whistleblower and suspected offender and other related persons.
3. Persons who, by virtue of the functions they exercise in the subject entity, namely under Article 26, become aware of any serious fact that includes the irregularities referred to in subsection 1 above, shall have the duty to report them to the supervisory organ, under the terms and with the safeguards established in this Article.
4. When no supervisory body is appointed, the communications referred to in the previous subsection shall be addressed to the management body of the subject entity.

5. The communications made under this Article, as well as the reports they give rise to, shall be conserved under the terms of Article 16 of the LPCBC-FT-PADM and placed at the permanent disposal of the CMC.
6. Subject entities shall refrain from any threats or hostile acts, and in particular any unfavourable or discriminatory labour practices against those making communications under this Article, and such communications shall not in themselves constitute grounds for the subject entity to initiate disciplinary, civil or criminal proceedings against the person making the communication, unless such communications are deliberate and manifestly unfounded.

Article 29.

(Implementation of restrictive measures)

1. For the purposes of the provisions of Article 24 of the LPCBC-FT-PADM, the subject entity shall adopt the necessary means and mechanisms to, as enforcement entity, ensure compliance with the obligations set out in Law 19/17 of 25 August on the Prevention and Combating of Terrorism and Law 1/12 of 12 January on the Designation and Execution of International Legal Acts.
2. For the purposes of the provisions of the preceding paragraph, the subject entity shall have permanent, prompt and secure mechanisms that ensure the immediate, full and effective execution of the restrictive measures, allowing, at least:
 - a) The detection of any persons or entities identified in restrictive measures;
 - b) The blocking or suspension of transactions or a set of transactions when the financial institution has to comply with the freezing obligations arising from the financial sanctions referred to in Article 24 of the LPCBC-FT-PADM; and
 - c) Immediately report to the competent authority, any frozen assets or other actions taken pursuant to the restrictive measures.

3. The subject entity monitors, through periodic independent evaluations, the proper functioning of the means and mechanisms implemented, aimed at ensuring compliance with the restrictive measures.
4. The Compliance Officer is responsible for:
 - a) Ensuring immediate and full knowledge and permanent updating of the lists of persons and entities issued or updated under the restrictive measures; and
 - b) Continuously monitoring the adequacy, sufficiency and timeliness of the means and mechanisms to ensure compliance with restrictive measures.
5. Whenever the subject entity decides not to proceed with the execution of restrictive measures, the Compliance Officer shall register it in a document or written record, in accordance with the provisions of the preceding paragraph:
 - a) The grounds for the non-execution decision; and
 - b) The reference to any informal contacts that may have taken place with the competent national authorities in the decision-making process, with an indication of their dates and the means of communication used.

Section IV

Obligation of Training

Article 30.

(Training of collaborators)

1. The subject entity shall define and apply an appropriate training policy for its managers, employees and other collaborators whose functions are relevant for the purposes of preventing and combating money laundering, financing of terrorism and the proliferation of weapons of mass destruction, aimed at ensuring full, permanent and updated knowledge on, among other aspects:

- a) The applicable legal framework on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;
 - b) The policies, procedures and internal controls on preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction defined and implemented by the subject entity;
 - c) Identification and reporting of transactions to the Compliance Officer;
 - d) Reporting of irregularities in accordance with the regulations;
 - e) The guidelines, recommendations and information issued by law enforcement authorities, supervisory authorities or industry representative associations;
 - f) The risks, types and methods associated with assets originating from or related to the commission of criminal activities or the financing of terrorism and the proliferation of weapons of mass destruction;
 - g) The vulnerabilities of the business areas developed, as well as of the products, services and operations made available by the entity, as well as the distribution channels of these products and services and the means of communication used with the clients;
 - h) The reputational, legal and prudential risks and the consequences of non-compliance with obligations to prevent and combat money laundering, the financing of terrorism and the proliferation of weapons of mass destruction; and
 - i) The specific professional responsibilities for preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction, and in particular policies, procedures and internal controls associated with the fulfilment of preventive and combating obligations.
2. In the case of newly hired employees whose duties are directly relevant to the prevention and combating of money laundering, terrorist financing and weapons of mass destruction proliferation, the subject entity, immediately upon their admission, shall provide them with adequate training on the policies, procedures and internal controls defined in

respect of the prevention and combating of money laundering, terrorist financing and weapons of mass destruction proliferation.

3. The records referred to in Article 23.2 of the LPCBC-FT-PADM contain at least the following information concerning the internal or external training activities that have been carried out:
 - a) Name and purpose of the training;
 - b) Date of training;
 - c) Training entity;
 - d) Duration in hours;
 - e) Nature, whether internal or external;
 - f) Environment, whether face-to-face or distance;
 - g) Supporting learning material;
 - h) Name and position of trainees, whether internal or external; and
 - i) Final evaluation of trainees, if any.

Section V

Reporting Obligation

Article 31.

(Declaration Form for Suspicious Transaction)

1. The suspicious transaction report, under the terms of Article 17 of the LPCBC-FT-PADM, must be made in physical or digital format, through a form to be addressed to the FIU.
2. The form referred to in the preceding number shall be approved by instruction of CMC.
3. A copy of any documents collected or records made shall accompany the suspicious operation report.
4. The duty to disclose set out in this Article covers the elements of the contractual relationship between the client and the entities subject to it, and the provisions of Article 25(2)(a) of the Portuguese Securities Code shall apply.

Article 32.

(Obligation of confidentiality)

1. The subject entities and the members of their governing bodies or persons exercising administrative, managerial or leadership functions in them, their employees, agents and other persons who render permanent, temporary or occasional services to them, shall not disclose to their customers their representatives or beneficial owners or third parties that the transaction was considered to reveal evidence of money laundering, financing of terrorism and proliferation of weapons of mass destruction and that, as a result, it was reported to the Financial Intelligence Unit.
2. The subject entities are also prevented from making available or allowing goods, operations or economic resources or other related services to be made available, directly or indirectly, for the benefit of:
 - a) Persons, groups and entities designated by the United Nations Sanctions Committee pursuant to United Nations Security Council Resolution 1267, as listed in the updated list of the said Sanctions Committee; and
 - b) States, persons, groups and entities designated in compliance with other international acts, under the terms of Article 6 of Law 1/12 of 12 January on the Designation and Enforcement of International Legal Acts, when applicable.

Section VI

Obligation to Cooperate

Article 33.

(Relationship with the National Designation Committee)

1. Without prejudice to other duties resulting from the Law, the subject entities shall cooperate with the National Designation Committee, under the terms foreseen in Law no. 1/12, of 12 January, of the Designation and Enforcement of International Legal Acts and in Presidential Decree No.

214/13 of 13 December, Regulating the Designation and Enforcement of International Legal Acts, as follows:

- a) To provide all necessary information requested by the National Designation Committee about its clients;
 - b) Check whether or not your clients are on the national list of designated persons, groups or entities;
 - c) Report to the competent authority and to the CMC whenever they hold assets owned, possessed or belonging to designated customers.
2. Subject entities shall not make available or permit to be made available assets or economic resources or transactions for the benefit of designated persons, groups or entities.

Section VII

Preservation Obligation

Article 34.

(Preservation of documents)

1. The subject entities shall ensure that all records of transactions and customers are available in a timely manner so that the competent authority, in accordance with the applicable law, can inspect them if it deems necessary.
2. The records shall be kept through the original documents, in the form of physical documents or through any other technological process, under the terms defined by the CMC.
3. The provisions of Article 16 of the LPCBC-FT-PADM apply to the retention of documents.

CHAPTER III

Supervision

Article 35.

(Selection of collaborators)

1. The subject entity must make a reasoned assessment of the reliability and credibility of the collaborators it intends to appoint for functions of greater sensitivity and risk in the full accomplishment of its activity, as well as its integrity.
2. The subject entity must also assess the reliability and credibility of the service providers it hires to perform services sensitive to its integrity and activity.
3. For the purpose of keeping documents resulting from the application of this article, the provisions laid down in paragraphs 2 and 3 of the preceding article shall apply, with the necessary adaptations.

Article 36.

(Checking the prevention system)

The CMC, within the scope of its supervisory powers, may, under the terms of the combined provisions of Paragraph 1(a) and Paragraph 2(c) of Article 57 of the LPCBC-FT-PADM and Article 33 of Law No. 1/12 of 12 January, of the Designation and Execution of International Legal Acts:

- a) To inspect the facilities of the entities subject without prior authorisation from them;
- a) To monitor compliance with the regulations contained in the LPCBC-FT-PADM;
- b) Check the system to prevent and combat money laundering, terrorist financing and the proliferation of weapons of mass destruction implemented by the subject entities, whenever they consider it necessary.

Article 37.

(Report on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction)

1. Subject entities shall annually send a specific report on their internal control system and other information to be defined by Ruling for the prevention and combat of money laundering, financing of terrorism and proliferation of weapons of mass destruction.
2. The report referred to in the previous number must be sent to CMC by 31 May of each year, covering the period between 1 January and 31 December of the previous year, and must follow the model to be defined by Instruction, which will also specify the terms for its submission.
3. The report comprises all information on:
 - a) Institutional information and relevant contacts of the subject entity;
 - b) The policies, procedures and internal controls on preventing and combating money laundering, the financing of terrorism and the proliferation of weapons of mass destruction;
 - c) Risk management;
 - d) Use of new technologies, products and services, with potential impact on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;
 - e) Monitoring compliance with the regulatory framework;
 - f) Control of compliance with the obligations related to the reporting of irregularities provided for in Article 8(1);
 - g) Internal audit;
 - h) External audit;
 - i) Information systems and tools;
 - j) Deficiencies detected by the subject entity on preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction;
 - k) Specific information on types of operations;
 - l) The corrective measures adopted to remedy the deficiencies identified by the subject entity and identified following supervisory actions undertaken by the CMC, if applicable;

- m) Relevant quantitative information;
 - n) Self-assessment questionnaire of the subject entity, with its perception as to the adequacy and degree of compliance of the procedures adopted in compliance with the Law and these Regulations and other relevant regulations; and
 - o) Other information relevant to the exercise of CMC's supervisory powers in the field of preventing and combating money laundering, terrorist financing and the proliferation of weapons of mass destruction.
4. Together with the information referred to in the previous number, the subject entities shall also report:
- a) The overall opinion of the management body on the adequacy and effectiveness of the respective internal control system, within the specific scope of preventing and combating money laundering, financing of terrorism and proliferation of weapons of mass destruction, in accordance with the risk assessment of the entity's activity;
 - b) Information on whether the supervisory body of the subject entity has detected any high-risk deficiencies in the internal control system for the prevention and combat of money laundering, financing of terrorism and proliferation of weapons of mass destruction of the subject entity during the reporting period;
 - c) Opinion of the supervisory body of the subject entity, expressing - in the negative and in a clear, detailed and reasoned manner - its opinion on the quality of the respective internal control system for the prevention and combat of money laundering, terrorist financing and the proliferation of weapons of mass destruction.
5. The subject entity shall update, on a permanent basis, the information referred to in paragraph 3(a), under the terms to be defined in specific regulations.

CHAPTER IV
Final Provisions

Article 38.

(Sanctions)

Infractions of the provisions of this Regulation shall be punishable under the terms of Law No. 5/20 of 27 January on the Prevention and Combating of Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction and, subsidiarily, the Portuguese Securities Code.

Article 39.

(Revocation)

Regulation no. 4/16, of 2 June, establishing the Conditions for Prevention of Money Laundering and Terrorist Financing, as well as any other regulation contradicting the provisions of this Regulation, is hereby repealed.

Article 40.

(Doubts and omissions)

The doubts and omissions arising from the interpretation and application of this Regulation shall be settled by the Board of Directors of the CMC.

Article 41.

(Entry into force)

This Regulation shall enter into force within 60 days after its publication.

Luanda, on 20 of October of 2021.

The President of the Capital Market Commission,

Maria Uini Baptista