AML/CTF/P Risk Management Policy

BIR BANK, S.A

Document Details

Title:	AML/CTF Risk Management Policies
File:	BIR_DCOMP_AML/CTF/P Risk Management Policies

Document Revision

Date:	Version	Responsible	Reason for intervention
11-2022	V4	DCOMP	Update
11-2022	V4	DORG	Configuration
12-2022	V4	IC	Validation

Approved by:

Date:	Version	Name	Signature
02-2023	V4	Board Management	

Sub-Process Updates:

Version	Date of entry into force	Amendments
V1	2015-12-04	Establishment (CA.OS.P.053.2015)
V2	2019-10-10	Layout Change (CA.OS.006.2019)
V3	2020-12-08	Addition of Notice 14/2020 and Law 5/20
V4	2023-02-27	Update

Legislation/Regulation to support the Sub-Process:

Diploma	Date of entry into force	Subject
Notice No 14/2020	22-06-2020	Anti-Money Laundering and Terrorist Financing Rules
Law No 14/21	28-01-2022	General Rules of Financial Institutions
Law No 5/20	27-01-2020	Prevention and Fight Against Money Laundering, Terrorist Financing and the Wide Spread of Weapons of Mass Destruction.
Notice No 01/2022	2022-01-28	Corporate Governance Code of Banking and Financial Institutions.

CONTENT

CHAPTER I - DEVELOPMENT, APPROVAL, REVIEW AND VALIDATION 6
I. PREPARATION, APPROVAL, REVIEW AND VALIDATION 6
CHAPTER II - SCOPE, IMPLEMENTATION AND OBJECTIVES OF THE POLICY 7
CHAPTER III - GENERAL PRINCIPLES 8
CHAPTER IV - ORGANIZATIONAL STRUCTURE - LINES OF DEFENSE 8
CHAPTER V - RISK MANAGEMENT MODEL 10
I. RISK-BASED APPROACH 10
II. RISK ASSESSMENT 11
III. CUSTOMER RISK EVALUATION 13
IV. MONITORING 13
V. CUSTOMER RISK MANAGEMENT 13
CHAPTER VI - TRAINING 14
ANNEX I - EXAMPLES OF POTENTIAL HIGH RISK FACTORS 17
I. CUSTOMER-RELATED RISK FACTORS 17
II. RISK FACTORS INHERENT TO PRODUCTS, SERVICES, TRANSACTIONS OR DISTRIBUTION CHANNELS 18
III. RISK FACTORS INHERENT TO GEOGRAPHIC LOCATION 19
IV. COMMUNICATION AND TRAINING 19
ANNEX II - ILLUSTRATIVE LIST OF POTENTIAL INDICATORS OF SUSPICION 21
I. GENERIC INDICATORS 21
II. INDICATORS RELATED TO CREDIT OPERATIONS 26
III. INDICATORS RELATED TO FUNDS TRANSFER OPERATIONS 27
IV. INDICATORS RELATED TO MANUAL EXCHANGE RATE OPERATIONS 29
V. INDICATORS RELATED TO EMPLOYEES OF FINANCIAL INSTITUTIONS 30
VI. OTHER INDICATORS 30
ANNEX III -GLOSSARY 32

CHAPTER I - DEVELOPMENT, APPROVAL, REVIEW AND VALIDATION

I. DEVELOPMENT, APPROVAL, REVIEW AND VALIDATION

This document must be formally approved by the Board of Directors and reviewed at least annually.

According to the Governance Policy of the Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (AML/CTF/P) Risk Management Model, the following Structural Units have responsibilities related to the AML/CTF Risk Management Policy of BIR:

Structure Unit	Responsibilities
Board of Directors (BD)	Approval of (AML/CTF/P), Risk Management Policy.
Executive Board (EB)	Definition of the Risk Strategy of BIR.
Directorate of Compliance (DCOMP)	Development and revision of the (AML/CTF/P), Risk Management Policy and submission to the BD Approval or equivalent body.
Directorate for Internal Audit (DIA)	Assessment of compliance with the (AML/CTF/P), Risk Management Policy.

CHAPTER II - SCOPE, IMPLEMENTATION AND OBJECTIVES OF THE POLICY

This document describes the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CTF) Risk Management Policy of *Banco de Investimento Rural* (hereinafter referred to as "BIR" or " Banco") regarding the management system for Anti-Money Laundering and Countering the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction, with the purpose of mitigating the risk of the Bank being used as a vehicle for criminal activities such as money laundering and terrorist financing through the products and services offered and reducing the likelihood of identified ML/CTF risks occurring, in order to protect the Bank from financial and reputational impacts and prevent the integration of illicit gains into the financial system, in accordance with Notice No. 14/20 of June 22, issued by the National Bank of Angola (hereinafter referred to as "BNA").

Therefore, and in compliance with the legal obligation imposed by Articles 14 and 22 of Law No 5/20 of 27 January and Articles 4 and 5 of Notice No 14/20, the Bank approves internal measures, procedures and programs for control and risk management training and enhanced due diligence aimed at ensuring the compliance of the acts of all its employees and auditors (internal and external) with the existing legal framework on the matter, of which are highlighted on Page No 4, as well as the 40 (forty) recommendations of the FATF/FATI (*FATF) Financial Action Task Force*) and the Basel Committee on the matter.

The Bank ensures that the results of the risk assessment are reflected and effectively implemented in existing internal risk management and mitigation policies and procedures. All relevant business units and/or employees are informed about the policies, procedures and any other risk management and mitigation measures identified.

The Bank carries out, whenever necessary, regular or extraordinary periodic tests of its risk management and mitigation measures, policies and procedures, and is subject to the oversight of internal control structures, including Compliance, Risk and Audit, and all the shortcomings identified in this context are known by the *Compliance Officer* for necessary adjustments.

This Policy is applied universally across all units and structures of BIR Bank and should be communicated to all employees. Recommendations of the International Financial Action Task Force - FATF AML/CTF Risk Management Policy.

CHAPTER III - GENERAL PRINCIPLES

The following general principles guide the BIR (AML/CTF), Risk Management Policy:

- **Transparency**: risk assessment and management are carried out in a transparent manner, creating evidence of intervention and decisions taken by different hierarchical levels, throughout the approval chain and the business relationship.
- **Segregation of Functions and Independence**: the assessment and monitoring of the level of risk exposure is carried out by an organizationally independent structure separate from the Bank's risk-assuming organizational structures, although these structures also have the responsibility to assess and monitor risks within their respective roles and competencies, with ultimate responsibility for risk management being the responsibility of the Board of Directors, which is to make available to the units and structures of BIR, the technical and human conditions for an adequate management of money laundering and defined terrorist financing risks.
- **Control**: The (AML/CTF) Risk Management System is subject to specific controls and is subject to independent testing, conducted by the Internal Audit Directorate (IAD), as a 3rd line of defence, independent of the structure.

CHAPTER IV - ORGANIZATIONAL STRUCTURE - LINES OF DEFENCE

Risk management is ensured through three (3) lines of defence at the level of its organizational structure:

LINES OF DEFENSE	STRUCTURE	RESPONSIBILITY

1th Line	Commercial Area/ Business Direction and Counters	• Identification of entities and verification *(Customer Due Diligence);*
		• Initial Risk Assessment:
		  ○ *KYC Scoring*
		  ○ Complementary due diligence measures according to the level of risk;
		• Approval hierarchy of entities (risk differentiated levels ensuring division of functions).

2th Line	Directorate of *Compliance* (DCOMP)	• Definition and revision of the KYC *Scoring* Model; • Implementation of Enhanced Due Diligence (EDD) measures according to the risk of entities; • Mandatory opinion on the approval of High Risk Classified Entities.
	Directorate Information Systems (DIS). Directorate of Risk Management (DRM).	• Ensuring data quality in Information Systems that serve as *input* to risk information systems. • Ensuring the definition and implementation of controls based on identified risks.
3th Line	Directorate Internal Audit (DIA)	• Ensuring independent validation and performance testing.

The responsibilities and competencies of the various units and structures of BIR within the scope of the AML/CTF/P Risk Management System are detailed in the "Anti-Money Laundering/Counter Financing of Terrorism Prevention Policies and Procedures Manual".

CHAPTER V - RISK MANAGEMENT MODEL

I. RISK-BASED APPROACH

The Bank develops an anti-money laundering risk rating system that applies to all customers and beneficial owners, which, operates in real time for the purposes of attribution of risk level, based on the weighting of the customers' known characteristics during the KYC procedure that are: professional activity, country of residence, expected transaction profile, politically exposed person status, etc.

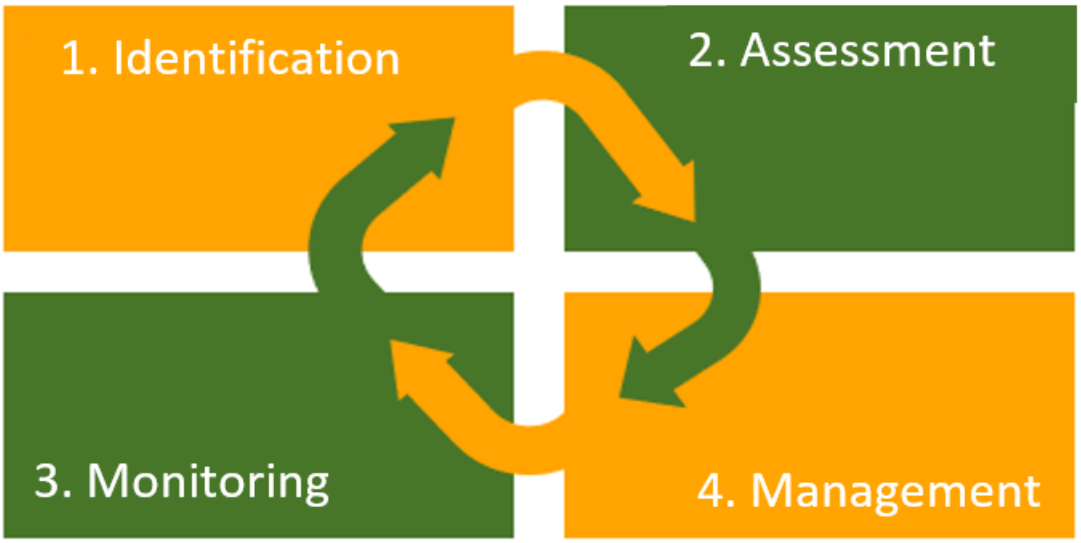
This system allows, through an automated *Scoring*, to assign each Customer an adjusted and differentiated level of risk.

As the process of classifying the money laundering risk of customers is dynamic, appropriate procedures should be applied to all existing customers and accounts based on the risk assigned to them or if their risk is increased according to the criteria determined by the Bank, in line with current legislation and regulations.

It is necessary to ensure that all transactions in existing active accounts are continuously monitored and any unusual or inappropriate pattern in their operation triggers a process of reassessing the customer's classification based on the update of their respective "Due Diligence."

In line with the above, adopting a risk-based approach has the following benefits, among others:

- Efficiency of the process for detecting entities and transactions suspected of ML/CTF;
- More effective risk and cost-benefit management;
- More efficient monitoring of identified threats and greater flexibility for the sector to adapt to the evolving risks over time.



II. RISK IDENTIFICATION

In identifying, assessing and mitigating of specific risks related to money laundering, terrorist financing, and proliferation of weapons of mass destruction, the Bank relies on reliable, credible, and diverse sources of information that provide information regarding their origin and nature. The main sources include:

- information, guidance or alerts issued or spread by the Banco Nacional de Angola (National Bank of Angola), related to typologies and methods of identifying specific or emerging risks or with suspicion indicators;

- information, guidance or alerts from the Financial Intelligence Unit ("FIU") or law enforcement authorities relating to typologies and methods for identifying specific or emerging risks or with suspicion indicators;

- Government information, guidance or warnings related to the prevention of money laundering and the financing of terrorism and the proliferation of weapons of mass destruction;

- Information derived from the national risk assessment;

- Lists drawn up by public bodies, in particular those of relevant political or public positions or of their holders;

- Internal analyses and documents, i.e., information collected during identification and due diligence procedures, as well as lists and databases internally prepared and updated by the *Compliance* and Risk Management Directorates;

- Independent and credible information from civil society or international organizations, on corruption indices, publicly disclosed documents, on levels of corruption and revenues associated with the performance of political or public positions in a given country or jurisdiction, as well as mutual evaluation reports from the Financial Action Task Force or its regional representations, and any other listings issued by relevant international organizations;

- Information from the Internet and media, provided that the source is independent and credible;

- Information contained in databases, lists, risk reports and other analyses from commercial sources available on the market;

- Official statistical data of national or international origin;

- Relevant academic research;

- Information made available by other Financial Institutions or Institutions of a similar nature, to the extent legally permissible;

- Information on the business area developed by customers, as well as the products, services and operations provided;

- Information about the history and nature of the Customer;

- The geographical location of the customer or the beneficial owner, as well as countries or geographical areas where the customer operates directly or through third parties, whether or not belonging to the same group, etc.

III. CUSTOMER RISK ASSESSMENT

The first step is to identify which ML/CTF risks affect the Bank. In the risk assessment it is necessary to consider the legal, regulatory and reputational aspects that may affect the BIR Bank.

- Customer Risk Assessment is performed using the KYC *Scoring* model developed by the Bank.
- The risk assessment is conducted at the time of account opening and throughout the business relationship, as part of periodic review and whenever an event triggers a re-evaluation, taking into account deficiencies identified at the internal control level.

IV. MONITORING

This stage ensures that the information produced in the previous stages is analysed in a timely manner by the relevant internal bodies, as well as reliable, complete and timely information on the risk exposure profile is communicated to external entities.

V. CUSTOMER RISK MANAGEMENT

Risk management relies on the development of mechanisms that enable risk exposure reduction and disclosure based on a robust integrated AML/CTF/P prevention program with a focus on the training programs based on the fight against ML/CTF, which aims to ensure the Bank's compliance with the applicable legal and regulatory framework, complying in particular with the

provisions of Article 23 of Law No 5/20 of 27 January and Article 25 of Notice No 14/20 of 22 June.

I. ORGANIZATIONAL MODEL:

STAGES OF RISK MANAGEMENT	RESPONSIBILITIES	KEY PLAYERS
Identification	Identify the ML/CTF risks to which BIR Bank is exposed	Management Board Executive Board *Compliance* Directorate
Assessment (Risk quantification)	Definition of Risk calculation matrices - development, revision of the *Scoring* methodology.	Management Board Executive Board *Compliance* Directorate
Monitoring	Development and implementation of measures to reduce risk exposure.	Management Board Executive Board Business Directorate *Compliance* Directorate Risk Direction
Management	Preparation and spreading of management information Independent evaluation	*Compliance* Directorate Directorate Internal Audit

CHAPTER VI - TRAINING

Without prejudice to the general obligation of risk management, training is essential in relation to the specific tasks carried out by the relevant staff in this field. The Bank pays special attention to the training of newly hired employees whose duties are directly relevant to the prevention of AML/CTF/P, on the basis of an integrated program of knowledge of policies, procedures and controls, ensuring that they do not start work without at least knowledge of:

- Basic principles and concepts regarding AML/CTF/P;
- The basic principles of the internal control system in place;
- Rules and procedures for implementing the principles identified above.

The training program includes classroom training, *on-job training* and/or *e-learning*.

Classroom and *on-job* training is mainly provided by in-house trainers, including the *Compliance Officer* and by people with high experience and training in the field, who are part of the Directorate of Compliance, and The Bank has defined and implemented an appropriate training policy for its managers, employees, and other collaborators in order to ensure comprehensive, ongoing, and up-to-date knowledge among other aspects:

a. the applicable legal framework and policies and procedures and controls on the prevention of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, implemented internally;
b. Identification and reporting of suspicious transactions to the *Compliance Officer*;
c. reporting of irregularities in accordance with the regulations;
d. guidelines, recommendations and information issued by law enforcement authorities, supervisors or industry associations;
e. the risks, typologies and methods associated with funds or other property derived from or related to the commission of criminal activities or to the financing of terrorism and the proliferation of weapons of mass destruction;
f. vulnerabilities in the business areas developed, as well as in the products, services and operations made available by the institution, as well as in the distribution channels for those products and services and the means of communication used with customers;

g. reputational, legal, and prudential risks, as well as the transgressive consequences resulting from non-compliance with the preventive obligations of Anti-Money Laundering, Counter Financing of Terrorism, and Proliferation of Weapons of Mass Destruction;

h. specific professional responsibilities in relation to the prevention of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, particularly pertaining to policies, procedures and controls associated with fulfilling preventive obligations.

ANNEX I - EXAMPLES OF POTENTIAL HIGH-RISK FACTORS

I.CUSTOMER-RELATED RISK FACTORS

1. Business relationships or occasional transactions that occur in unusual circumstances, in view of the Customer's expected profile and other elements characterizing the business relationship or occasional transaction.
2. Customers/beneficial owners who are resident or active in the countries or jurisdictions referred to in the following paragraphs 20 to 26.
3. Legal persons or legal arrangements which are vehicles for the holding of personal assets.
4. Companies with *nominee shareholders* or whose registered capital is represented by bearer shares.
5. customers that are engaged in cash intensive transactions.
6. Ownership or control structures of the Customer (in particular its chain of interests, domain or control) that appear unusual or excessively complex in view of the nature of the activity pursued by the Customer.
7. Politically Exposed People (PPEs).
8. Correspondents' resident in third countries.
9. Beneficial owners who have been subject to sanctions or restrictive measures imposed by the United Nations Security Council or by the European Union;

non-profit organizations where:

a) The organization represents, at the domestic level, a significant proportion of the financial resources controlled by the non-profit sector.

10. The organization represents a significant proportion of the international activities carried out by the non-profit sector. For these purposes, the activity carried out through:
    a. branches or subsidiaries outside the organization itself;
    b. associated non-profit organizations, including their branches and subsidiaries outside such organizations;

c. the ownership or control structure or organizational model appears unusual or excessively complex, taking into account the nature of the activity pursued.

11. Business relations, occasional transactions or operations in general expressly indicated by the Banco Nacional de Angola (National Bank of Angola), depending on the risks associated with Customers/Beneficial owners.

II. RISK FACTORS INHERENT TO PRODUCTS, SERVICES, TRANSACTIONS OR DISTRIBUTION CHANNELS

1. Private *Banking*.
2. *Trade Finance* - Commercial Finance.
3. Products or transactions which may favour anonymity.
4. Business relationships or occasional transactions established/executed using means of distance communication.
5. Payments received from third parties unknown or unrelated to the Customer or the activity it pursues.
6. Products made available and transactions carried out in a banking correlation table with credit institutions established in third countries.
7. New products and new business practices, including new distribution mechanisms and payment methods, as well as the use of new technologies or technologies under development for both new and existing products.
8. Business relations, occasional transactions or operations in general expressly indicated by the Banco Nacional de Angola (National Bank of Angola) in relation to risks associated with products, services, transactions or distribution channels.

III. RISK FACTORS INHERENT TO GEOGRAPHICAL LOCATION

1. Countries or jurisdictions with strategic deficiencies in the field of AML/CTF/P prevention, identified by the Financial Action Task Force in a document published by this body on the website with the address.
2. Other countries or jurisdictions identified by credible sources (such as publicly disseminated evaluation/monitoring reports) as lacking effective systems to prevent money laundering or terrorist financing.
3. Countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activities.
4. Countries or jurisdictions that have been subject to countermeasures decided by the Council of the European Union.
5. Countries or jurisdictions subject to sanctions, embargoes or other restrictive measures imposed inter alia by the United Nations Security Council and the European Union.
6. Countries or jurisdictions providing financing or support for terrorist activities, or in whose territory known terrorist organizations operate.
7. *Offshore* centres.
8. Business relations, occasional transactions or operations in general, expressly indicated by the Banco Nacional de Angola (National Bank of Angola), depending on risks associated with geographical factors.

IV. DISSEMINATION AND TRAINING

Without prejudice to the general obligation of administration, training is essential in relation to the specific tasks carried out by the relevant staff in this field. The Bank pays special attention to the training of newly hired employees whose duties are directly relevant to the prevention of ML/CTF, on the basis of an integrated program of knowledge of policies, procedures and controls, ensuring that they do not start work without at least knowledge of:

- Basic principles and concepts regarding AML/CTF/P;

- The basic principles of the internal control system in place;
- Rules and procedures for implementing the principles identified above.

The training program includes classroom training, *on-job training* and/or *e-learning*.

Classroom and *on-job* training is mainly provided by in-house trainers, including the *Compliance Officer* and by people with high experience and training in the field, who are part of the Directorate of Compliance, and The Bank has defined and implemented an appropriate training policy for its managers, employees, and other collaborators in order to ensure comprehensive, ongoing, and up-to-date knowledge among other aspects:

i the applicable legal framework and policies and procedures and controls on the prevention of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, implemented internally;

j Identification and reporting of suspicious transactions to the Compliance Officer;

k. reporting of irregularities in accordance with the regulations;

l. guidelines, recommendations and information issued by law enforcement authorities, supervisors or industry associations;

m. the risks, typologies and methods associated with funds or other property derived from or related to the commission of criminal activities or to the financing of terrorism and the proliferation of weapons of mass destruction;

n. the vulnerabilities of the business areas developed, as well as the products, services and operations provided by the institution, as well as the distribution channels for those products and services and the means of communication used with customers;

o. reputational, legal, and prudential risks, as well as the transgressive consequences resulting from non-compliance with the preventive obligations of Anti-Money Laundering, Counter Financing of Terrorism, and Proliferation of Weapons of Mass Destruction;

p. specific professional responsibilities in relation to the prevention of money laundering, the financing of terrorism and the proliferation of weapons of mass destruction, particularly pertaining to policies, procedures and controls associated with fulfilling preventive obligations.

ANNEX II - ILLUSTRATIVE LIST OF POTENTIAL INDICATORS OF SUSPICION

I.GENERIC INDICATORS

1. Customers who carry out occasional transactions (any transaction conducted by the subject entities outside the scope of an established business relationship) or engage in operations that, due to their nature, frequency, amounts involved, or any other risk factor, are inconsistent with their usual profile.
2. Customers who move cash without a plausible explanation:
    a. in unusual amounts;
    b. In amounts not justified by the Customer's profile;
    c. unusually packaged;
    d. in a poor state of repair; or
    e. Represented by small denomination banknotes, in order to exchange them for high denomination banknotes.
3. Customers who in any way seek to persuade employees of the financial institution not to comply with any legal obligation or internal procedure regarding the prevention of ML/CTF.
4. Customers who show reluctance or refuse to provide identification documents, supporting evidence, or other information, or fail to carry out the necessary verification procedures deemed necessary by the financial institution in order to:
    a. Identify the Customer, its representative or the beneficial owner;
    b. Understand the Customer's ownership and control structure;
    c. Have knowledge of the nature and purpose of the business relationship;
    d. Have knowledge of the origin and destination of the funds; or
    e. The characterization of Customer activity.
5. Customers who are reluctant or refuse to provide original or equivalent documents.
6. Customers who are reluctant or refuse to update their information.

7. customers who are reluctant or refuse to make face-to-face contact with the financial institution.
8. Customers providing identifiers, supporting evidence or other items of information:
    a. not very credible as to its authenticity;
    b. Not very clear about their content;
    c. difficult for the financial institution to verify; or
    d. With unusual features.
9. Customers who present different identification documents each time they are requested by the financial institution.
10. customers who, in the course of their business, use aliases, nicknames or any other alternative expression to their real name or denomination.
11. Customers who postpone or fail to provide documentation that can be submitted to the financial institution at a time after the establishment of the business relationship.
12. Customers seeking to suspend or modify the business relationship or occasional transaction after being asked for their identification document, the supporting evidence or other information relevant to the Customer's knowledge.
13. Customers who do not wish to send any correspondence to the declared address.
14. Customers with no apparent relationship to each other, providing common addresses or contact details (telephone number, fax number, e-mail address or other).
15. customers whose address or contact details (telephone number, fax number, e-mail address or other) are incorrect or permanently inoperative, in particular where the financial institution's attempt to contact them takes place shortly after the establishment of a business relationship.
16. Customers whose address or contact details (telephone number, fax number, e-mail address or other) change frequently.
17. customers who appear to be acting on behalf of a third party but do not disclose it to the financial institution or, even if they do disclose it, refuse to provide the necessary information about the third party on whose behalf they are acting.

18. Customers who seek to establish close relations with employees of the financial institution.
19. Customers seeking to restrict any contacts they establish with the financial institution to a specific employee or employees of the financial institution, in particular when - in the absence of such employee or employees - the Customers decide not to perform or suspend operations.
20. Customers who have unusual knowledge of money laundering and terrorist financing legislation.
21. Customers who show an unusual interest and curiosity in knowing the financial institution's internal control policies, procedures and mechanisms aimed at preventing ML/CTF.
22. Customers who have entered into similar business relationships with different financial institutions in a short period of time.
23. customers operating in successive different locations in an apparent attempt to avoid detection by third parties.
24. Customers who repeatedly carry out transactions below the thresholds that would require identification procedures.
25. customers who acquire significant assets and who, within a short period of time and for no apparent reason, sell them.
26. Customers conducting transactions at different establishments of the institution on the same day or within a reduced period of time.
27. Customers who provide unclear or inconsistent explanations about transactions or who have little knowledge about their purpose.
28. Customers who provide excessive and unsolicited explanations about transactions.
29. Customers who are experiencing nervousness or an abnormal urgency in the execution of operations.
30. customers related to suspicious ML/CTF transactions reported by the financial institution to the competent authorities.

31. Customer involved in suspicious ML/CTF transactions reported by supervisory authorities under Articles 17 and 19 of Law No 5/20 of January 27th and known to the financial institution.
32. Customers who are or have been under scrutiny for engaging in criminal activities, in particular ML/CTF/P or any of the criminal offenses underlying these two types of crimes (such information being either directly known to the financial institution or acquired through a credible public source).
33. Customers expressly referred to by the competent authorities as being potentially related to AML/CTF/P operations.
34. Customers engaged in any kind of financial activity without being duly authorized or entitled to do so.
35. transactions which show a degree of complexity that is apparently unnecessary for the achievement of their intended purpose, owing in particular to the number of financial movements, financial institutions, accounts, persons involved and/or countries or jurisdictions involved.
36. operations whose purpose or economic logic is not evident.
37. transactions where the frequency, and unusual nature does not explain the customer's profile.
38. Operations that appear to be inconsistent with the current practice of the Customer's business or business sector.
39. transactions involving shadow companies.
40. Transactions that have no connection with the Customer's known activity and that involve persons or entities related to countries or jurisdictions publicly recognized as:
    a. drug production/trafficking sites;
    b. holders of high levels of corruption;
    c. money laundering platforms;
    d. promoters or supporters of terrorism; or
    e. Promoters or supporters of the proliferation of Weapons of Mass Destruction.

41. Transactions that have no connection with the known activity of the Customer and that involve persons or entities related to the countries, territories or regions with privileged tax regimes or other countries or jurisdictions with strongly restrictive banking secrecy legislation.
42. business relationships or occasional transactions that seek to disguise the identity of beneficial owners, including through complex corporate structures.
43. customers holding a significant number of open bank deposit accounts, in particular when some of them remain inactive for a long period of time.
44. Customers with bank deposit accounts with several credit institutions located in the same country/geographical area.
45. Customers making deposits without knowing the exact amounts to be deposited.
46. Customers who open accounts with large amounts of cash.
47. Customers who frequently use personal accounts to perform transactions that relate to their business.
48. Accounts in which there are frequently movements for which the account holder does not provide a credible justification.
49. Accounts opened at counters geographically distant from the Customer's home or workplace.
50. Accounts whose activity greatly exceeds that which would be expected at the time of their opening.
51. Accounts which consist of or are maintained by a large number of persons who have no personal or professional relationship with each other.
52. Accounts held by legal persons which pursue economic activities which are unrelated to each other, all of which are held by the same natural persons.
53. Accounts moved through a large number of small claims and a small number of large claims.
54. Accounts with frequent cash credits and/or debits, and such movement is not consistent with the Customer's profile or with its business or business sector.

55. Accounts in which frequent deposits are made by persons with no apparent personal or professional relationship with the holders of those accounts.
56. accounts which are used to pool funds from other accounts, subsequently transferred on block, in particular when such transfer occurs outside the national territory.
57. Accounts showing, for no apparent reason, a sudden increase in movements, movements and/or average balances.
58. Inactive accounts for a long period with sudden movements of large amounts or movements via cash deposits.
59. Accounts used almost exclusively for transfers of funds from and to the outside.
60. Accounts held by entities domiciled in *offshore centres* and sharing the same beneficial owner, with frequent and complex movements of funds recorded among these accounts.
61. Accounts with large and frequent deposits exclusively through automated teller machines or night-time deposit boxes, in particular where deposits are in cash.
62. Accounts which are the subject of cash deposits immediately after the holders have access to the hire safe which they hold with the financial institution.

II. INDICATORS RELATED TO CREDIT OPERATIONS

1. Early repayment of loans when they are made:
    a. unexpectedly and for no apparent logical reason;
    b. to the economic detriment of the borrower;
    c. with funds from third parties;
    d. Using funds of uncertain origin and inconsistent with the Customer's profile;
    e. using funds transferred from accounts held with more than one financial institution; or
    f. By the use of cash (in particular in the context of consumer credit transactions).

2. Request for credit without apparent economic justification for the transaction, taking into account, for example, the high value of the assets held by the Customer.
3. Request for credit from Customers who do not show any concern in discussing the terms of the transaction, in particular the costs associated with it.
4. Request for credit based on guarantees or assets deposited with the financial institution, own or third parties, whose origin is unknown and whose value is not in line with the financial situation of the Customer.
5. Request for credit from Customers who are already borrowers of loans granted by institutions domiciled in *offshore centres* and that have no connection with the known activity of Customers.
6. Request for credit from Customers who declare to the financial institution income with origin not fully clarified by its holders.
7. Request for credit from Customers who propose, as a counterpart to the approval of the same, the application of large sums in the constitution of deposits or other products.
8. A credit application where the borrower's documentation to be part of the borrower's process is made available to the financial institution by a third party with no apparent relationship to the transaction.
9. Absence of evidence of the use of the borrowed amounts, the Customer withdrawing in cash the amount credited to its bank deposit account and corresponding to the loan granted.
10. making credit card payments and payments repeatedly made by persons other than the cardholder.

III. INDICATORS RELATED TO FUNDS TRANSFER OPERATIONS

1. Segmented transfers in several transactions in order to avoid the fulfilment of legal and regulatory obligations foreseen for transactions reaching a certain amount.
2. Transfers abroad that are inconsistent with the known activity of the Customer, due to, inter alia, the amount, frequency or beneficiaries of such transfers.
3. transfers in which - at any time in the distribution of funds, including when the funds are made available to their final recipients - persons or entities are involved, in any capacity, formally or informally, who are not duly authorized to carry out such activity by the competent authorities of the countries or jurisdictions concerned.
4. Transfers where there is no apparent connection between the known activity of the Customer and the payers/payees of the transactions or the countries/geographical areas of origin/destination of the transactions.
5. Transfers where the Customer refuses or is reluctant to provide an explanation for the operation.
6. Transfers to or from a payer for which the Customer discloses little or reluctant information.
7. Transfers for amounts greater than those expected when establishing the business relationship with the Customer.
8. Outward transfers to a wide range of beneficiaries who do not appear to have family links with the Customer.
9. Transfers made to a wide range of beneficiaries, these being nationals of countries or jurisdictions known to be involved in terrorist activities.
10. Transfers ordered regularly by the same person or entity, the recipients being different from each other and the amounts transferred being equal to or close to each other.
11. Transfers ordered regularly by the same person or entity, the recipient being common and the amounts transferred being different.
12. Transfers ordered by different persons or entities and sent to the same beneficiary on the same or very similar date.

13. Transfers ordered by different persons or entities having in common one or more pieces of personal information (surname, address, employer, telephone number), made on the same or very close dates.
14. Transfers ordered by different persons or entities, with funds made available by only one of them.
15. Transfers from funds provided by a third party.
16. Large transfers with instructions to make funds available to the cash recipient.
17. Off-site transfers in which the transferred amounts immediately leave the Customer's account or, if there is no account, are immediately transferred to other recipients.
18. Transfers accompanied by instructions to make the amounts transferred available to third parties and not to the beneficiaries of the operations.
19. External transfers, cross - checked with transfers from the outside for the same values or approximations.
20. Transfers where Customers show unusual interest and curiosity about the funds transfer system, such as operating procedures and/or limits.
21. Transfers abroad, carried out at times apparently not coinciding with the payment of wages, in particular when ordered by immigrant citizens.

IV. INDICATORS RELATED TO MANUAL EXCHANGE RATE OPERATIONS

1. Segmented transactions into multiple purchases/sales to avoid legal and regulatory obligations for transactions up to a certain amount.
2. Transactions that are inconsistent with the known activity of the Customer, due to, inter alia, the amount or frequency of such transactions.
3. Transactions executed on the basis of an exchange rate more favourable to the financial institution than the advertised rate and/or the payment of commissions at a higher amount than due, on the proposal of the Customer.
4. Transactions where Customers wish to exchange large sums in a given foreign currency for another foreign currency.

5. Transactions with non-resident Customers who appear to be traveling to the domestic territory for the express purpose of making purchases/sales of currency.
6. Frequent operations with low denomination banknotes or low international currency.
7. Transactions where Customers instruct the financial corporation to subsequently surrender the consideration to a third party.
8. Transactions in which Customers insist on receiving the consideration by check from the financial institution, and this practice is not usually adopted by the financial institution.
9. Transactions where Customers request to receive the foreign currency equivalent of banknotes with the highest possible face value.
10. Operations where Customers request the receipt of the equivalent in several postal vouchers of reduced amounts, on the order of several beneficiaries.

V. INDICATORS RELATED TO EMPLOYEES OF FINANCIAL INSTITUTIONS

1. Employees who repeatedly fail to comply with legal obligations or internal procedures regarding the prevention of AML/CTF/P.
2. Employees who establish with Customers familiarity and proximity relationships that go beyond the normal standard in the context of the functions assigned to them or are inconsistent with the internal practices of the financial institution.
3. Employees exhibiting a pattern of social behaviour or other external signs not commensurate with the financial situation of the employees as known by the financial institution.

VI. OTHER INDICATORS

1. transactions relating to the sale of real estate where:
    a. the sale value is much higher than the market value;
    b. payment is made by bearer check or by an endorsed check to a third party which has no apparent connection with the transaction;

c. the payment is made in cash, in particular from a bank deposit account held by a third party which has no apparent relationship with the buyer; or

d. the immovable property transacted was recently purchased by the seller.

2. Operations related to non-profit organizations where:

   a. the nature, frequency or number of operations is not consistent with the size of the organization, its objectives and/or its known activity;

   b. the frequency and number of operations is suddenly increased;

   c. the organization maintains large funds in its bank deposit account for long periods;

   d. the organization only solicits contributions from persons or entities not resident in Angola;

   e. the organization appears to have little or no human and logistical resources allocated to its activity;

   f. the representatives of the organization are not resident in Angola, in particular where large amounts are transferred to their country of residence;

   g. The organization has some kind of connection with countries or jurisdictions publicly recognized as drug production/trafficking sites, as having high levels of corruption, as money laundering platforms, as promoters or supporters of terrorism, or as promoters or supporters of the proliferation of weapons of mass destruction.

3. Customers who suddenly substantially increase the number of visits to their rental vaults.
4. Customers making high-value transactions through prepaid cards or acquiring a prepaid card payment from the same financial institution.

ANNEX III -GLOSSARY

AML (*Anti-money laundering*) - Anti-Money Laundering.

Anti-Money Laundering and Counter Terrorism Financing* (AML/CTF) *Policy - Anti-Money Laundering and Counter Terrorism Financing Compliance Policy.

CTF (*Counter-Terrorism Financing*) - Countering Terrorism Financing.

Due Diligence - Enhanced Due Diligence.

E-Learning - E-led learning, usually the Internet.

Enhanced Due Diligence - enhanced due diligence.

***Financial Action Task Force* (FATF)** - Financial Action Task Force.

On-*job* training - On-site or job training.

TF (*Terrorism financing*) - Terrorism financing.

***Know your Customer* (KYC)-**Know your customer.

ML (*Money Laundering*) - Money laundering.

Mobile Banking - Electronic Banking Service in Mobile Phones/Smartphone.

OFAC (*Office of Foreign Assets Control*) - U.S. Department of Foreign Assets Control.

Offshore - Fiscal Paradise.

Online - Available to access.

Private ***Banking***.

Risk Based Approach - Risk Based Approach.

Shareholders - Shareholders.

Site - Page/Site on the Internet.