POLICY FOR THE PREVENTION OF MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM ("PBC/CFT")

September 2025

ATLANTICO EUROPA

CONTENTS

Framework 3
1. Introduction 3
2. Regulations 4
2.1. Relevant rules 4
3. Concepts 5
4. Duties 11
5. Misdemeanour liability 15
Internal policies and procedures 18
1. Organisation and risk management 18
2. Staff training 21
3. Control Processes 22
4. Identification and knowledge of clients 25
5. Politically Exposed Persons 37
6. Control and conservation of documentation 38
7. Analysing and controlling operations 38
8. Reporting suspicious transactions 40
Approval, Communication and Review 43
1. Approval and communication 43
2. Review 43
Annexes 48

FRAMEWORK

1. Introduction

Banco Atlântico Europa ("the Bank") considers the active prevention of money laundering and terrorist financing ("ML/TF") to be a fundamental principle of its business, adopting the practices implemented in the Portuguese market, in accordance with the legislation and respective regulations in force in Portugal, as well as internationally recognised practices.

The Bank adopts a policy of co-operation with the authorities responsible for combating money laundering and terrorist financing.

In order to comply with the legal and regulatory standards to which it is subject, the Bank has adopted internal rules and procedures that enable it to get to know its customers and the activities they carry out, as well as those that enable it to carry out its banking and financial activities in accordance with strict ethical rules.

This Policy applies to all the Bank's Employees, and may be extended to subsidiaries, branches and representative offices of the Bank and its employees, where they exist, to the extent that it is approved by the respective bodies and, where necessary, adapted to local law, legislation and regulations.

Regulations

The rules and procedures contained in this Policy are mandatory in nature and must at all times be fully observed by the Bank's employees, as well as by its external employees, advisors and third parties acting on behalf of the Bank.

This Policy has been drawn up to promote compliance with the legal and regulatory provisions in force and the internal rules additionally established by the Bank in the field of preventing money laundering and combating the financing of terrorism ("AML/CFT"), and no recipient of this document is exempt from consulting the legal rules or guidelines in force to which it refers.

1. Relevant rules

Internationally:

a. 40 FATF recommendations, revised in 2017 (where the 9 recommendations on combating terrorist financing are integrated);

b. Regulation (EU) 2015/847 of the European Parliament of 20 May (on information accompanying transfers of funds);

c. Regulation (EC) No 881/2002, as amended by Commission Implementing Regulation (EU) 2017/1834 of 9 October (establishes measures to combat terrorism directed against certain persons and entities);

d. Regulation (EC) No 2580/2001, as amended by Council Implementing Regulation (EU) 2017/965 of 8 June (laying down measures against certain persons and entities).

e. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May on the prevention of the use of the financial system for the purpose of BC&FT.

In the national sphere:

a. Law 83/2017 of 18 August (on the prevention of money laundering and terrorist financing);

b. Law 52/2003 of 22 August: approves the law on combating terrorism.

c. Law no. 89/2017 of 21 August (on the Central Registry of Beneficial Owners);

d. Ministerial Order no. 292/2011, of November 8, as amended by Ministerial Order no. 345-A/2016, of December 30 (which approved the list of countries, territories and regions with clearly more favourable privileged taxation regimes);

e. Banco de Portugal Notice no. 1/2022 (on the conditions of exercise, procedures, instruments, mechanisms, application formalities, reporting obligations and other aspects necessary to ensure

compliance with the duties to prevent money laundering and terrorist financing, within the scope of the activity of financial entities subject to Banco de Portugal supervision);

f. Instruction 8/2024 (defines the information to be reported annually to the Bank of Portugal by the financial entities subject to its supervision);

g. Bank of Portugal Circular Letter 91/2006/DSB (on non-cooperative countries and territories);

h. Law no. 97/2017 of 23 August on the application and enforcement of restrictive measures approved by the UN or EU;

i. Good practices regarding the implementation of Bank of Portugal restrictive measures;

2. Concepts

Money laundering

Under the terms of article 368a of the Penal Code, "money laundering" means any activity aimed at: converting, transferring, assisting or facilitating any operation of conversion or transfer of advantages, obtained by oneself or a third party, directly or indirectly, with the aim of concealing their illicit origin, or preventing the perpetrator or participant in such offences from being criminally prosecuted or subjected to a criminal reaction. In addition, the punishment is extended to anyone who conceals or disguises the true nature, origin, location, disposition, movement or ownership of the advantages, or the rights relating to them.

"Advantages" are considered to be assets derived from the commission, in any form of co-participation, of the typical illicit acts of pimping, sexual abuse of children or dependent minors, extortion, trafficking in narcotics and psychotropic substances, arms trafficking, trafficking in human organs or tissues, trafficking in protected species, tax fraud, influence peddling, corruption and other offences referred to in the measures to combat organised and economic-financial crime, and typical illicit acts punishable by a prison sentence of a minimum of more than 6 months or a maximum of more than 5 years, as well as the assets obtained from them.
In addition to the above, Law 83/2017 also establishes that money laundering is understood to be the acquisition, possession or use of assets, with knowledge, at the time of receipt, that they come from a criminal activity or participation in an activity of that nature , as well as participation in one of the acts referred to in the preceding paragraphs, the association to carry out said act, the attempt and complicity in its carrying out, as well as the fact of facilitating its execution or advising someone to carry it out.

Terrorism

Under the terms of Law no. 52/2003, of 22 August, "Terrorism" means any concerted action aimed at undermining national integrity and independence, preventing, altering or subverting the functioning of state institutions provided for in the Constitution, forcing a public authority to carry out an act, to refrain from carrying it out or to tolerate it being carried out, or intimidating certain people, groups of people or the population in general, by means of:

a. An offence against the life, physical integrity or liberty of persons;

b. A crime against the security of transport and communications, including computer, telegraphic, telephone, radio or television communications;

c. The offence of intentionally creating a common danger by fire, explosion, release of radioactive substances or toxic or asphyxiating gases, flood or avalanche, collapse of a building, contamination of food and water intended for human consumption or the spread of a harmful disease, pest, plant or animal;

d. Acts that destroy or make impossible the operation of, or divert from their normal purposes, permanently or temporarily, totally or partially, means of communication or communication routes, public service installations or installations intended to supply and satisfy the vital needs of the population;

e. Research and development of biological or chemical weapons;

f. Crimes involving the use of nuclear energy, firearms, biological or chemical weapons, explosive substances or devices, incendiary means of any kind, packages or booby-trapped letters, whenever, by their nature or the context in which they are committed, these crimes are likely to seriously affect the State or the population they are intended to intimidate.

Effective Beneficiary

Under the terms of Law no. 83/2017 and Bank of Portugal Notice no. 5/2015, a Beneficial Owner is any natural person on whose behalf a transaction or activity is carried out or who ultimately owns or controls the Client.

Beneficial Owner of Corporate Entities

In cases where the Client is a corporate entity which does not have shares admitted to trading on a regulated market (or which is subject to information disclosure requirements equivalent to those required by European Union Law), the following persons are considered to be Effective Beneficiaries:

a. The natural person or persons who ultimately hold direct ownership or control of a sufficient percentage of shares or voting rights or participation in the capital of a legal person. For these purposes, evidence of direct ownership is considered to exist in cases where a natural person holds shares representing more than 25 per cent of the Client's share capital;

b. The natural person or persons who ultimately hold indirect ownership or control of a sufficient percentage of shares or voting rights or participation in the capital of a legal person. For these purposes, indications of indirect ownership are the holding of shares representing more than 25 per cent of the Client's share capital by:

    - A corporate entity that is under the control of one or more natural persons; or
    - Several corporate entities under the control of the same natural person or persons.

c. The natural person or persons exercising control by other means over that legal person;

d. The natural person or persons who hold the top management position, if, after all possible means have been exhausted and provided there are no grounds for suspicion:

e. no person has been identified pursuant to the preceding subparagraphs; or

f. there are doubts that the person or persons identified are the beneficial owners.

Beneficial Ownership of *Trusts* and other non-corporate legal persons

When the Client is a trust or other legal person of a non-corporate nature, the following are considered to be Effective Beneficiaries:

a. The *settlor* (*settlor*, in the case of *trusts*);

b. The trustee or trustees of trusts, or their administrators in the case of other non-corporate legal persons;

c. The trustee, if applicable;

d. The beneficiaries or, if they have not yet been determined, the category of persons in whose main interest the *trust* or non-corporate legal person was set up or carries out its activity;

e. Any other natural person who has ultimate control of the *trust* or non-corporate legal person, through direct or indirect participation or by other means.

Politically Exposed Persons

Qualified as Politically Exposed Persons (PEP) are natural persons who hold, or have held up to one year ago, in any country or jurisdiction, the following prominent public functions at a senior level:

a. Heads of State, Heads of Government and members of the Government, namely Ministers, Secretaries and Under-Secretaries of State or equivalent;

b. Deputies or other members of parliamentary chambers;

c. Members of the Constitutional Court, the Supreme Court of Justice, the Supreme Administrative Court, the Court of Auditors, and members of supreme courts, constitutional courts, courts of auditors and other high-level judicial bodies of other states and international organisations;

d. Representatives of the Republic and members of the self-government bodies of autonomous regions;

e. Ombudsman, Councillors of State, and members of the National Data Protection Commission, the Superior Council of the Judiciary, the Superior Council of Administrative and Tax Courts, the Attorney General's Office, the Superior Council of the Public Prosecutor's Office, the Superior Council of National Defence, the Economic and Social Council, and the Regulatory Entity for the Media;

f. Heads of diplomatic missions and consular posts;

g. General Officers of the Armed Forces and the National Republican Guard (GNR) in effective service, as well as the Chief Superintendents of the Public Security Police (PSP);

h. Presidents and councillors with executive functions of municipal councils;

i. Members of the management and supervisory bodies of central banks, including the European Central Bank;

j. Members of the administrative and supervisory bodies of public institutes, public foundations, public establishments and independent administrative bodies, however appointed;

k. Members of the management and supervisory bodies of entities belonging to the public business sector, including the business, regional and local sectors;

l. Members of the executive management bodies of national or regional political parties;

m. Directors, deputy directors and members of the board of directors or persons exercising equivalent functions in an international organisation;

n. Members of the European Parliament;

o. Public managers and members of the management body of a public limited company who exercise executive functions;

p. Members of the management body of a company in which the State has a stake, when appointed by the State;

q. Members of the management bodies of companies in the regional or local business sectors;

r. Members of the governing bodies of public institutes;

s. s) Members of the board of directors of an independent administrative body;

t. Holders of 1st and 2nd degree senior management positions, and equivalent, and senior managers of municipal council services and municipalised services, where these exist.

For the purposes of the declaratory obligations set out in this policy, the following are considered to be holders of senior public office:

u. a) The chiefs of staff of the members of the national and regional governments;

v. b) Representatives or consultants mandated by the governments of the Republic and regional governments in processes of concession or disposal of public assets.

Close family members" means:

a. Relatives and relatives up to the 2nd degree, in the straight or collateral line, of a politically exposed person;

b. Spouses or unmarried partners of a politically exposed person;

c. Unmarried partners of the politically exposed person's relatives referred to in point a), insofar as they do not enjoy the status of affinity;

d. Persons occupying similar positions in other legal systems.

Persons recognised as closely associated" means:

a. Any natural person who is known to co-own, with a politically exposed person, a legal person or a centre of collective interests without legal personality;

b. Any natural person who owns the share capital or voting rights of a legal person, or the assets of a centre of collective interests without legal personality, known to have a politically exposed person as their beneficial owner;

c. Any natural person known to have a corporate, commercial or professional relationship with a politically exposed person.

Holders of other political or public office" means:

Natural persons who, not being qualified as politically exposed persons, hold or have held, in the last

12 months and in national territory, the positions listed in articles 2 and 3 of Law no. 52/2019, of 31 July, which approves the regime for the exercise of functions by holders of political office and high public office.

It should be understood that the PEP category applies to persons residing in Portugal and outside Portugal.

Occasional transaction

Any transaction carried out by obliged entities outside the scope of an already established business relationship, characterised in particular by its occasional nature.

Unacceptable customers

The Bank does not accept the opening of accounts for unidentified Customers or numbered accounts, nor does it accept the opening of accounts for processes that show signs of fraud. In addition, the following are considered unacceptable BC/FT risk Clients:

a. Clients related to countries, entities or individuals sanctioned by the UN, the European Union, among others;

b. Clients who show suspicious behaviour or strange questioning;

c. Client(s) and/or their associated entity(ies) (in the case of legal persons: representatives, shareholders, beneficial owners/ senior management, directors) are referenced in ML/TF databases;

d. The existence of records of attempted fraud or other risky behaviour in the Customer's history of interactions;

e. Clients or entities that have already been Clients whose accounts have been closed for compliance reasons;

f. Shell banks;

g. Anonymous entities, or those controlled by anonymous individuals;

h. Lack of information on the nature and purpose of the business and the origin and destination of the Client's funds;

i. Clients who use their account with the Bank to trade virtual assets.

Any exceptions to the above must be submitted in advance to the Compliance Department for consideration and subject to approval by the Bank's Executive Committee.

3. Duties

The Bank is obliged to fulfil the following duties:

3.1 Duty of identification and diligence

It is the Bank's duty to identify Customers, whether natural or legal persons, whether they are owners or representatives, and verification must be carried out by means of original supporting documents in accordance with the legislation in force. The entire account opening process and supporting documents will be filed in the systems established for this purpose.

It is also the Bank's duty to identify the parties when carrying out an occasional transaction.

3.2 Due diligence procedures in addition to identification

The Bank must also adopt due diligence procedures in addition to the duty of identification on a regular basis and according to the degree of risk of each Customer.

3.3 Duty of refusal

The Bank must refuse to enter into business relationships, carry out occasional transactions or carry out other operations when:

a. Do not obtain the identifying information and the respective means of proof relating to the Client, their representative and/or Beneficial Owner;

b. Do not obtain the information necessary to ascertain the status of Beneficial Owner and the Customer's ownership and control structure;

c. Do not obtain information on the nature, object and purpose of the business relationship;

d. Is unable to carry out the procedures necessary to fulfil the duty to update.

The Bank must include in a document or written record the possible reasons for the impossibility of complying with the due procedures, as well as the grounds for any termination of business relationships already established, and also mention any consultations with the authorities, indicating the respective dates and means of communication used.

3.4 Duty to keep documents

Documents proving identification, as well as any other documents recording transactions that allow them to be reconstructed, must be kept, under the terms of article 51 of Law 83/2017, for a period of

7 years from their execution, even if the business relationship has already ended.

The Bank must keep copies of all communications made under the duty of communication for a period of 7 years from the moment the communication is made.

Without prejudice to the provisions of the preceding paragraphs, the Bank shall, in any case, adopt all necessary measures in order to respond fully to requests for information from the authorities aimed at determining whether it maintains, or has maintained in the last 10 years, business relations with a given natural, legal or similar person, and the nature of these relations.

3.5. Duty of scrutiny

The Bank must analyse with special attention transactions which, due to their nature, complexity, purpose, unusual nature of the Customer's way of operating, amounts involved, frequency, economic and financial situation of the Customers involved or the means of payment used and the profile of those involved, are likely to be related to money laundering or terrorist financing.

For the purposes of the previous article, the Bank will take particular account of the following characterising elements:

a. The nature, purpose, frequency, complexity, unusualness and atypicality of the conduct, activity or operations;

b. The apparent lack of an economic objective or lawful purpose associated with the conduct, activity or operations;

c. The amounts, origin and destination of the funds handled;

d. The place of origin and destination of the transactions;

e. The means of payment used;

f. The nature, activity, operating pattern, economic and financial situation and profile of those involved;

g. The type of transaction, product, corporate structure or centre of collective interests without legal personality that may particularly favour anonymity.

3.6 Duty to report

The Bank must immediately inform the Central Department of Investigation and Criminal Action ("DCIAP") of the Attorney General's Office ("PGR") and the Financial Intelligence Unit ("UIF") whenever it knows, suspects or has sufficient reason to suspect that certain funds or other assets, regardless of the amount involved, come from criminal activities or are related to terrorist financing. The Compliance

Officer monitors these communications.

The Bank, as a Credit Institution, must also immediately inform the Attorney General of the Republic and the other competent national authorities whenever it becomes aware or suspects that an act or omission has taken place or is taking place that could constitute a violation of a restrictive measure, under the terms of Law 97/2017, of 23 August ("Law 97"). The Bank must also report, on a systematic basis, to the DCIAP of the PGR and to the UIF, or any other types of operations that may be defined by specific regulations.

The form, deadline, content and other terms of the systematic communications made by the Bank must be in accordance with the legislation in force.

Decisions not to exercise the duty of communication shall be critically reviewed on a monthly basis by the Director responsible for regulatory compliance, and the results of this review shall be presented to the Board of Directors.

3.7 Duty to abstain and suspension decisions

The Bank must refrain from carrying out operations that it knows or suspects are related to the commission of money laundering or terrorist financing offences.

The Bank shall immediately fulfil its duty to report (under the terms referred to above regarding the duty to report) when it refrains from carrying out any operation, informing the authorities of the grounds for refraining.

The Bank may only carry out the operations for which it has exercised the right to abstain when:

a. The Bank is not notified, within seven (7) working days of the aforementioned communication, of DCIAP's decision to temporarily suspend the operation;

b. The Bank is notified, within the period referred to in the previous paragraph, of DCIAP's decision not to order the temporary suspension of the operation, under the terms of the law, which may be executed immediately.

If the Bank considers that refraining from carrying out the operation is not possible, or if, after consulting the PGR and the UIF, it is judged that it may hinder the investigation and prosecution of the beneficiaries of the operation, the operation may be carried out and the bank must immediately provide the PGR and the UIF with information about it, and this documentation must be kept for a minimum period of 7 years and made permanently available to the sectoral authorities.

If notified of DCIAP's decision to temporarily suspend the operation, the Bank must suspend the operation until it is subject to judicial review, which will decide whether or not to maintain the temporary suspension of the operation.

3.8. Duty to co-operate

The Bank shall provide all assistance required by the DCIAP, the PGR and the UIF, and by the other competent judicial and police authorities or by the authorities responsible for supervising and overseeing compliance with legally established duties.

3.9. Duty of non-disclosure

The Bank, the members of its governing bodies, persons exercising directorial, managerial or supervisory functions, as well as its employees, agents and other persons providing services to the Bank may not disclose to the Client or third parties that a criminal investigation is underway or that legally due information on a transaction has been transmitted.

The Bank ensures that any necessary contacts with Customers relating to communications arising from criminal investigations or enquiries are carried out, where appropriate and proportionate, in liaison with the Compliance Officer and, where necessary, with the competent judicial or police authorities.

3.10. Duty of control

The Bank must adopt internal control, risk assessment and management, internal auditing and communication policies and procedures that enable it to fulfil the legal duties to which it is subject and are capable of preventing the carrying out of operations related to money laundering and terrorist financing.

3.11. Training obligation

The Bank must implement training mechanisms so that all its directors and employees are aware of the obligations to which the Bank is subject in the area of preventing money laundering and terrorist financing and are able to recognise operations that may be related to this type of illicit activity.

The Bank ensures that the people referred to in the previous paragraph are given specific and regular training appropriate to each sector of activity, enabling them to recognise operations that may be related to money laundering and terrorist financing.

In the case of newly hired employees whose duties are directly related to the prevention of money laundering and terrorist financing, the Bank must provide them with appropriate training on the policies, procedures and controls defined internally for this purpose.

Training shall be provided by persons or entities with recognised competence and experience in the field of preventing and combating money laundering and terrorist financing, and shall be preceded by

a favourable opinion from the Regulatory Compliance Officer.

The Bank will keep an up-to-date and complete record of the training activities carried out, preserving it for a period of 7 years from the date it was carried out and making it permanently available to the sectoral authorities.

3.12. Obligations in the field of data protection and processing

The Bank is authorised to carry out the processing of personal data necessary to fulfil its legally prescribed duties.

The exclusive purpose of the Bank's processing of personal data is to prevent money laundering and the financing of terrorism, and such data may not be processed for any other purpose, including commercial purposes, without prejudice to other laws applicable to the processing of personal data.

The Bank ensures that personal data is deleted as soon as the retention periods associated with the retention obligation (7 or 10 years, see "Retention obligation") have elapsed.

3.13. Specific obligations

As a financial organisation, the Bank is particularly obliged to comply with the following:

a. The opening, maintenance or existence of anonymous accounts is not permitted, nor is the use of fictitious names or denominations;

b. Enhanced due diligence measures must be applied to cross-border correspondent banking relationships with institutions established in third countries, obtaining information on the nature of their activity, internal control processes in terms of money laundering and terrorist financing and the characteristics of their supervision;

c. Whenever the Bank establishes correspondence relationships involving institutions established in third countries, it must put in writing the respective responsibilities of each institution;

d. It is forbidden to establish correspondence relationships with shell banks;

e. The Bank also complies with the procedure for freezing funds laid down in Article 16 of Law No. 97.

4. Liability

Without prejudice to criminal liability for the offence of money laundering to which both natural and legal persons may be subject (see Article 368-A and Article 11 of the Penal Code), or other related sanctioning provisions applicable to each specific case, there are administrative offences for failure to

comply with the duties and obligations imposed by Law 83/2017, for which they may be held liable:

a. Financial entities;

b. Non-financial obligated entities;

c. Natural persons who hold administrative, managerial, directorship, leadership or supervisory positions, representatives, workers or other employees, whether permanent or occasional.

The liability of the legal or similar person is only excluded when the agent acts against its express orders or instructions.

Failure to comply with the duties and obligations imposed by Law 83/2017 is punishable by administrative offence.

Within the scope of the Bank's activity, the following fines may be imposed as a penalty:

€ 50,000.00 to € 5,000,000.00, if the perpetrator is a legal person or an entity assimilated to a legal person;

€ 25,000.00 to € 5,000,000.00, if the perpetrator is a natural person.

Outside the scope of the Bank's activity, but still within the scope of the activity of another financial entity, the following fines may be imposed as a penalty:

€ 25,000.00 to € 2,500,000.00, if the agent is a legal person or an entity assimilated to a legal person;

€ 12,500.00 to € 2,500,000.00, if the perpetrator is a natural person.

If the above limits are lower than 10 per cent of the Bank's total annual turnover, that percentage of total annual turnover will become the limit for the fines in question.

The following measures may also be applied as ancillary sanctions:

i. Forfeiture in favour of the State of the object of the offence and the economic benefit obtained by the agent through its commission; Prohibition, for a period of up to three years, of the exercise of the profession or activity to which the administrative offence relates;

ii. Closure, for a period of up to two years, of the establishment where the agent carries out the profession or activity to which the administrative offence relates;

iii. Prohibition, for a period of up to three years, from exercising the profession or activity to which the administrative offence relates;

iv. Inhibition, for a period of up to three years, from exercising functions of administration, management, leadership, ownership of corporate bodies, representation, mandate and supervision in entities subject to the supervision or supervision of Banco de Portugal and in entities with which they are in a control or group relationship;

v. Publication of the final or res judicata decision.

INTERNAL POLICIES AND PROCEDURES

1. Organisation and Risk Management

1.1 Those responsible for the Bank's business and support areas are also responsible for:

a. Implementing, controlling and verifying the degree of compliance with the prevention and control procedures in their organisational unit, keeping the Compliance Department informed.

b. Being aware of and monitoring incidents related to money laundering and terrorist financing in their organisational unit, keeping the Compliance Department informed.

c. Suggesting and implementing, in collaboration with the Compliance Department, the additional control procedures and precautionary measures it deems necessary, based on the specifics of its organisational unit, with the aim of detecting and preventing suspicious operations.

1.2 The Bank's Board of Directors is responsible for implementing and applying policies, procedures and controls on the prevention of money laundering and terrorist financing:

a. Approving the policies and internal procedures and controls appropriate to the Bank's activity, as well as updating them, being responsible in particular for reviewing and updating this Policy on an annual basis;

b. Having adequate knowledge of the money laundering and terrorist financing risks to which the Bank is exposed, as well as the processes used to identify, assess, monitor and control these risks;

c. Ensure that the Bank's organisational structure allows for the proper implementation of policies and appropriate procedures and controls at all times, preventing conflicts of interest and, where necessary, promoting the separation of functions within the organisation;

d. Promote a culture of prevention of money laundering and terrorist financing that encompasses all the Bank's employees whose functions are relevant for the purposes of preventing money laundering and terrorist financing, underpinned by high standards of ethics and integrity and, where necessary, the definition and approval of appropriate codes of conduct;

e. Appointing the Regulatory Compliance Officer;

f. Monitor the activities of other members of senior management, insofar as they oversee business areas that are or may be exposed to money laundering and terrorist financing risks;

g. Periodically monitoring and assessing the effectiveness of the policies, procedures and controls approved and implemented, ensuring that the appropriate measures are taken to correct any shortcomings detected.

1.3 It will be the responsibility of the Regulatory Compliance Officer to:

a. Participating in defining and issuing a prior opinion on policies and procedures and controls aimed at preventing money laundering and terrorist financing;

b. Continuously monitoring the suitability, sufficiency and up-to-dateness of policies, procedures and controls on the prevention of money laundering and terrorist financing, proposing the necessary updates;

c. Participating in defining, monitoring and evaluating the Bank's internal training policy;

d. Ensuring the centralisation of all relevant information from the Bank's various business areas;

e. Playing the role of interlocutor with the judicial, police, supervisory and inspection authorities, namely by complying with the Bank's duty to communicate and ensuring the exercise of other obligations to communicate and collaborate with the relevant authorities.

1.4. The Regulatory Compliance Officer must:

a. Perform his/her duties independently, permanently, effectively and with the decision-making autonomy necessary for such performance, whatever the nature of his/her relationship with the Bank;

b. Have the appropriate suitability, professional qualifications and availability to carry out the job;

c. Have adequate technical, material and human resources and means, including the employees necessary for the proper performance of the job;

d. Have unrestricted and timely access to all internal information relevant to the performance of their duties, in particular information relating to the fulfilment of the duty of identification and diligence and the records of operations carried out;

e. Not be subject to potential functional conflicts, especially when their duties are not segregated.

1.5. The Bank also appoints a member of the management body responsible for monitoring compliance with ML/TF regulations, ensuring that he or she:

a) Has the necessary knowledge to fully understand the matters covered by these functions;
b) Carries out these duties with the availability, decision-making autonomy and resources necessary for their proper performance;
c) Has unrestricted and timely access to all information and internal documentation relevant to the performance of these duties;
d) Performs these functions with an adequate segregation of potentially conflicting duties, ensuring that any situations of potential conflicts of interest are identified in advance, minimised and subject to careful and independent monitoring.

1.6. The Internal Audit Department is responsible for regularly monitoring and testing the design, efficiency and effectiveness of the Bank's AML/CFT programme, thereby also providing additional

assurance to the Board of Directors on these matters.

The Head of the Internal Audit Department is responsible for:

a. Monitoring the performance of the functional areas and the Compliance Department; and,

b. Carrying out design and effectiveness tests on controls within the scope of PBC/CFT.

c. To this end, the Bank must:

d. Continuously assess the applicability of the procedures in force;

e. Define and monitor the main risks and respective indicators associated with BC/FT;

f. Ensure an effective training strategy; and,

g. Periodically carry out effectiveness tests on the procedures and systems adopted.

In addition, in order to obtain a more in-depth and independent view of the effectiveness and efficiency of the BCP/CFT Programme, the Bank should also regularly promote specialised external audits on these matters.

The Compliance Department carries out periodic and independent prior control and/or a posteriori monitoring of the quality, suitability and effectiveness of the policies, procedures and control systems adopted with regard to the prevention of money laundering and terrorist financing. This control is carried out in parallel with the work carried out by the internal audit function and the external auditors.

1.7 The Bank's Board of Directors, together with the Compliance Department, identify the specific risks of money laundering and terrorist financing that exist in the context of the Bank's specific operating reality, including the risks associated with:

a. The nature, size and complexity of the activity pursued by the Bank;

b. Its customers;

c. The business areas developed, as well as the products, services and operations made available by the Bank, with particular attention to the risks that may arise from offering products or operations that may favour anonymity;

d. New commercial practices, distribution mechanisms or payment methods, as well as the use of new technologies in new or pre-existing products;

e. The distribution channels for the products and services provided, as well as the means of communication used to contact customers;

f. The countries or territories of origin of the obligated entity's Customers, or where they are domiciled or otherwise carry out their business;

g. The countries or territories in which the obligated entity operates, directly or through third

parties, whether or not they belong to the same group;

The Bank will take into account the degree of probability and impact of each of the risks specifically identified, and the overall risk of the Bank and its business areas.

For the purposes of complying with the previous paragraph, the Bank's Board of Directors shall meet with the Compliance Department in order to assess the ongoing suitability of the procedures for mitigating the specific money laundering and terrorist financing risks to which the Bank is subject and, where applicable, propose and approve changes to the internal regulations relating to money laundering and terrorist financing matters.

The Head of the Compliance Department provides the Bank's Board of Directors and Executive Committee with a quarterly report on its activity, including the work and controls carried out during the reference period in relation to the money laundering and terrorist financing risks identified, the effectiveness of the procedures implemented and, where applicable, suggests additional mechanisms suitable for mitigating new risks that are identified.

The Bank's Board of Directors will provide the Compliance Department with adequate material and human resources so that it is properly equipped to fulfil its duties in a swift, informed and independent manner.

1.8. The Bank's Employees play an important role with regard to AML/CFT. As such, all the Bank's Employees are responsible for ensuring that they comply with the provisions of this Policy.

In carrying out their daily duties, Employees must:

a. Remain vigilant to the possibility of BC/FT situations occurring;

b. Immediately report any suspicions of ML/TF to the Compliance Department;

c. Comply with all procedures relating to identifying Clients, opening and maintaining accounts, monitoring accounts, maintaining and recording documentation, and co-operating in providing information to the Compliance Department; e,

d. Ensuring that Clients are not alerted to any reports to the authorities about their transactions.

Employees are also responsible for completing all PBC/CFT training assigned to them, and subsequently diligently applying the knowledge acquired in such training, in accordance with their respective roles/responsibilities.

2. Staff training

All the Bank's employees who are directly or indirectly involved in issues related to the prevention of money laundering and terrorist financing will be given specific training courses on the matter in

question, which will be supervised by the Compliance Department . Training sessions are held every 2 years at the most and whenever there are new regulations that justify it.

In the case of newly hired employees whose duties are directly related to the prevention of money laundering and terrorist financing, the Bank, after their admission and up to a maximum of 6 months, provides them with adequate training on the policies, procedures and controls internally defined on the prevention of money laundering and terrorist financing.

To the extent necessary, the Compliance Department and the Legal Department may develop training and clarification tools on the subject of the prevention of money laundering and terrorist financing and the measures adopted by the Bank, and the Bank's employees will be notified of any changes to this Policy via a dedicated platform on the Bank's Intranet.

At the end of each training course, trainees must be assessed in order to verify the knowledge they have acquired.

The Bank guarantees that the duty to provide training is complied with under the same terms in its group relations or with branches and subsidiaries, and must, to the extent applicable and whenever justified, take into account the local legislation in which they are located.

3. Control Processes

The Bank adopts internal control mechanisms and procedures for assessing and managing ML/TF risk, complemented by a communication system (internal and to legal authorities), in order to mitigate or prevent this risk.

For control purposes, the Bank must continually ensure the applicability of the procedures in force, defining and monitoring the main ML/TF indicators and risks.

3.1. Evaluation of ML/TF risks

The Bank is responsible for adopting internal control, risk assessment and management, internal auditing and communication mechanisms and procedures that enable it to fulfil the legal duties to which it is subject, and that are capable of preventing the occurrence of operations related to ML/TF.

The Bank adopts internal control mechanisms and procedures for assessing and managing the risk of compliance in PBC/CFT, complemented by a communication system (internal and to legal authorities), in order to mitigate or prevent this risk. The design of the processes includes the primary activities aimed at executing operations, identifying and accepting those involved, as well as the control activities carried out by the execution areas, the Compliance Department and the Internal Audit Department.

Other factors that are appropriate to the Bank's operating reality should also be taken into account, and the isolated presence of factors and types indicative of risk does not necessarily determine the automatic attribution of a high or low degree of risk to the business relationship or occasional transaction.

To this end, the Bank defines its controls based on an annual assessment of its exposure to ML/TF risks. The risk assessment methodology is based on a set of risk factors defined by the Bank.

The Bank's risk is mitigated by the PBC/CFT internal control system.

The Compliance Department is responsible for carrying out the risk assessment. If the assessment identifies that certain risks are not being adequately mitigated, the Compliance Department must propose an action plan to implement new controls and/or review existing ones.

The decision to manually review the degrees of risk is always substantiated and is the responsibility of the Compliance Officer or another Bank employee who is not directly involved in the commercial relationship with the client, under their supervision.

The Bank must ensure that it has all the relevant information about the people and entities with which it has dealings. In this way, the Bank must ensure that it adopts a risk-based due diligence methodology. With this approach, counterparties with high BC/FT risks should be considered high risk and enhanced due diligence and monitoring should be carried out. The Bank should regularly update counterparty due diligence information during the business relationship to ensure accurate risk classification. Due diligence should be reviewed if any event indicates that the risk associated with the client has changed (e.g. blocked or even rejected transactions, or negative information from public information sources). In the case of clients classified as high risk, due diligence should be reviewed at least every two years.

3.2 Filtering system

Screening plays an important role in identifying the risks associated with ML/TF. As such, the Bank must implement controls to filter out Customers and their relevant related parties (e.g. BEFs, representatives, proxies, among others), Transactions and Suppliers, in line with the provisions of this Policy and the Sanctions Policy.

The automatic filtering systems used by the Bank must fulfil the minimum requirements of *fuzzy matching*. This mechanism allows for the setting of a matching percentage, whereby only alerts with a level of similarity greater than the defined value will be investigated, thus allowing for the assignment of a probabilistic classification for each case resulting from the filtering. The filtering systems must be calibrated in accordance with the Bank's risk assessment.

The Bank's filtering systems take into account the most up-to-date lists of PEP Clients and Sanctions,

namely the UN, the European Union, etc., as well as the list of "Bad Guys", which also includes entities publicised by the Bank of Portugal.

Filtering should be carried out on:

a. All new customers and their relevant related parties, suppliers and employees;

b. All existing customers of the Bank at least monthly;

c. When there are changes to counterparty information;

d. When new additions are made to the Sanctions and WBS Client lists; e,

e. Transfers and payments issued/received from customers to/from other banks.

For the purposes of this Policy, it should be emphasised that, in addition to the possible self-declaration of a client as a PEP, it is the filtering system that acts as an identification check on PEP clients for the subsequent enhanced due diligence process. In the same context, this is the system used to identify sanctioned parties with whom the Bank cannot establish business relations or, if these relations pre-exist the sanction, they must be frozen and reported to the competent authorities.

3.3 Client Risk Classification

The Bank's reputational defence and PBC/CFT processes, framed within a logic of differentiation and graduation of BC/FT risk, only become truly effective with the application of classification, analysis and monitoring policies that make it possible to permanently understand the entity's level of risk.

In these circumstances, the Bank monitors the risk level of its customers on a daily basis and uses different criteria - which vary according to the type of customer - to classify them:

The risk levels currently in force are as follows: High, Medium, Low.

The procedure for assigning the risk level is automatic and is based on information that is taken daily from each customer's database, with a relative weight being assigned to each eligible risk criterion. The criteria selected by the Bank vary depending on whether the client is a company or a private client and relate to elements of the client's connection to risk factors (professional activity, political relations, place of residence, nationality, jurisdiction of activity, among others).

The Bank internally assigns a different weight to each of these risk factors, using an automatic weighting formula which results in a corresponding automatic risk level classification.

The level of risk attributed to each entity only influences the risk to be attributed to the customer, and there is no equivalence of risk between entities belonging to the same customer. Only entities classified as PEP contribute to increasing the risk of the entities involved in the same client.

During the business relationship established with customers or guarantors, the Bank carries out periodic and non-periodic diligence and procedures with the aim of ensuring that the information it already has is up-to-date, accurate and complete. The period for updating data is directly linked to the customer's risk level, with the following criteria:

- High (1): annually or after the expiry date;
- Medium Risk (2): every 3 years or after the expiry date; and,
- Low Risk (3): every 5 years or after the expiry date.

4. Customer Identification and Knowledge

Considering that knowing the customer is a fundamental tool in the fight against the use of the financial system for money laundering and terrorist financing, the Bank undertakes to only start a business relationship with customers who provide the information required by law and after analysing this information.

The Bank has developed the account opening process in such a way as to allow all information about the Client, as well as their Beneficial Owners (if applicable), to be collected and registered prior to the start of the business relationship with the Client. All relevant identification data must always be verified by means of original supporting documents or certified copies, of which the Bank must keep copies.

The Compliance Department may order the collection of additional information when the Customer presents additional potential risk factors, taking into account *Know Your Customer* information.

The identification and due diligence procedures set out in this chapter regarding Customers and their representatives, as well as their Beneficial Owners, must be complied with whenever the Bank:

a. Establishes business relationships (a relationship of a commercial or professional nature that is expected to be or is of a lasting nature);

b. Carries out occasional transactions of an amount equal to or greater than €15,000, either through a single operation or through several operations that appear to be related to each other;

c. You suspect that the transactions, regardless of their value and any exception or threshold, may be related to money laundering or terrorist financing;

d. You have doubts about the veracity or adequacy of the customer identification data previously obtained.

4.1 Identifying information

When identifying natural persons, the following elements will be collected:

a. Photograph;

b. Full name;

c. Signature;

d. Date of birth;

e. Nationality on the identification document;

f. Type, number, expiry date and issuing organisation of the identification document;

g. Tax identification number or equivalent issued by a competent foreign authority;

h. Occupation and employer, if any;

i. Full address of permanent residence and, where different, tax residence;

j. Place of birth;

k. Other nationalities not listed on the identification document.

l. In the case of legal representatives or agents of customers, the Bank also checks the document authorising such persons to act on their behalf.

When identifying legal persons or collective interest centres without legal personality, the following elements are collected:

i. Name;

ii. Object;

iii. Full address of the registered office and, where applicable, of the branch or permanent establishment or any other address of the main places of business;

iv. Legal person identification number or equivalent issued by a competent foreign authority;

v. Identity of the holders of shareholdings and voting rights equal to or greater than 5%;

vi. Identity of the members of the management body or equivalent, as well as other relevant senior executives with management powers;

vii. Country of incorporation;

viii. CAE code, institutional sector code or other code of a similar nature, if available.

4.2 Evidence of identity

Natural Persons:

For the purposes of verifying the identification of natural persons, the presentation of an original, valid identification document issued by a competent public body should always be required, with a photograph, showing the full name, signature, date of birth and nationality.

Legal persons and collective interest centres without legal personality ("similar entities"):

For the purposes of verifying the identification of legal persons, a certificate from the commercial register should always be required or, in the case of an entity with its registered office located outside national territory, an equivalent document issued by an independent and credible source, which includes the name, purpose, full address of the registered office (and where applicable, the branch or permanent establishment) and the legal person identification number (or equivalent in the case of an entity with its registered office abroad).

4.3 Time of identity verification

Except in the cases listed below for situations in which it is exceptionally possible to verify identity after the relationship has begun, identity verification is carried out before the business relationship is established or any occasional transaction is carried out.

Identity verification may only be completed after the start of the business relationship, but as soon as possible, provided that the following conditions are met cumulatively:

a. If this is necessary in order not to interrupt the normal course of business;

b. The contrary does not result from a legal or regulatory rule applicable to the Bank's activity;

c. The situation in question presents a low risk of money laundering and terrorist financing, expressly identified as such by the Bank;

d. The Bank implements the appropriate measures to manage the risk associated with that situation, in particular by limiting the number, type or amount of transactions that can be carried out.

4.4 Due diligence procedures in addition to identification

The Bank must also, on a regular basis and depending on the degree of risk of each Customer:

a. Take appropriate measures to understand the Client's ownership and control structure, in particular with a view to ascertaining the status of Beneficial Owner (where applicable);

b. Obtain information on the purpose and intended nature of the business relationship;

c. Obtain information on the origin and destination of the funds handled within the scope of a business relationship or when carrying out an occasional transaction, when the Customer's risk profile or the characteristics of the operation justify it;

d. Continuously monitor the business relationship in order to ensure that such transactions are in line with the organisation's knowledge of the Client's activities and risk profile;

e. Keeping the information obtained during the course of the business relationship up to date, which must be updated at least every five years in the case of lower risk, every 3 years in the case of medium risk and annually in the case of high risk.

f. Whenever the risk analysis carried out by the Bank on the business relationship or occasional transaction warrants a greater degree of knowledge of the Customer, their representative or the beneficial owner, the Bank will request additional information or elements to the extent appropriate to the risk specifically identified.

4.5 Duties relating to Beneficial Owners

Prior to establishing a business relationship or carrying out any occasional transaction (and with the exception of the cases listed above), the Bank assesses the status of the beneficial owner and collects at least the identifying information described above, whenever:

a. The Client, their beneficial owners, the business relationship or operation represent an increased risk of money laundering or terrorist financing;

b. The beneficial owner(s) is (are) the natural person(s) who holds the top management position of the Client;

c. When they act as *trustees* or perform a similar function in *express trusts* or collective interest centres with a similar structure or functions; or

d. This is determined by specific regulations or by decision of the competent sectoral authorities.

In addition, the Bank must:

i. Consult the information collected on beneficial owners in the central register of beneficial owners, whenever the Client, under the terms of Law no. 89/2017, is obliged to register its beneficial owners in national territory;

ii. Carry out these consultations at intervals appropriate to the specific risks identified and, at least, whenever they carry out, update or repeat the identification and due diligence procedures provided for in this policy;

iii. Make the establishment or continuation of the business relationship or occasional transaction dependent on verification of compliance with the registration obligation, when due under the terms of Law no. 89/2017;

iv. Immediately notify the Institute of Registry and Notary Public (Instituto de Registos e Notariado, I.P.) of any discrepancies between the identification contained in the central register and that

resulting from compliance with the identification and diligence duties provided for in this policy.

The Bank will also comply with the provisions of the preceding articles whenever the Customer is a natural person who may not be acting on their own account.

4.6 Duty of identification in occasional transactions

Before carrying out an occasional transaction for an amount greater than €15,000.00, the Bank must collect and record all information about the Client and their Beneficial Owners (if applicable). All relevant identification data must always be verified by means of original supporting documents or certified copies, of which the Bank must keep copies.

The Bank will check that the identification details submitted are up to date, regardless of whether they have already been collected when carrying out a previous occasional transaction.

Whenever the Bank proposes to carry out, in person or by means of remote communication, occasional transactions of an amount equal to or greater, in national or foreign currency, than the equivalent of €15,000.00, regardless of whether the transaction is carried out through a single operation or several operations that appear to be related to each other, or occasional transactions of any amount for which it has suspicions of a possible relationship with ML/TF offences, the Bank must obtain at least the identification details of the Customers and their representatives at the beginning and during the operation.

4.7 Simplified identification and due diligence measures

The Bank may simplify the measures adopted under the duty of identification and due diligence when it identifies a demonstrably low risk of money laundering and terrorist financing in business relationships, occasional transactions or operations.

The adoption of simplified due diligence measures is only admissible following a risk assessment by the Bank itself or by the Bank of Portugal.

Simplified measures may never be adopted in any of the following situations:

a. When there are suspicions of money laundering or terrorist financing;

b. When enhanced identification or due diligence measures must be adopted;

c. Whenever determined by the Bank of Portugal.

These situations are indicative of potentially lower risk:

Reduced risk factors inherent to the Client:

- Companies with shares admitted to trading on a regulated market and subject, by virtue of the rules of that market, the law or other binding instruments, to information duties that guarantee adequate transparency as to the respective beneficial owners;
- Public administrations or companies;
- Customers living in lower risk geographical areas, as determined in accordance with Law 83/2017.

Reduced risk factors inherent to the product, service, operation or distribution channel:

- Limited and clearly defined financial products or services aimed at increasing the level of financial inclusion of certain types of Customers;
- Products in which the risks of money laundering and terrorist financing are controlled by other factors, such as the imposition of load limits or transparency of ownership, which may include certain types of electronic money.

Examples of simplified measures are:

i. Reducing the frequency of updates to the identification elements collected;

ii. Reducing the intensity of continuous monitoring and the depth of analysis of transactions when the amounts involved are small in relation to the customer's profile;

iii. Failure to collect specific information and to implement specific measures to understand the purpose and nature of the business relationship, when it is reasonable to infer the purpose and nature of the relationship from the characteristics of the transaction itself.

The simplified measures to be applied by the Bank must be proportionate to the reduced risk factors identified.

4.8 Reinforced identification and due diligence measures

The Bank shall reinforce the measures adopted under the duty of identification and diligence when the Bank or the Bank of Portugal identifies an increased risk of money laundering or terrorist financing in business relationships, occasional transactions or operations.

For the purposes of adopting reinforced measures, the Bank must define different degrees of risk that reflect its specific operating reality, taking into account at least the following aspects:

- The nature, size and complexity of its business;
- The respective customers;
- Business areas developed, as well as the products, services and operations provided;
- Distribution channels for the products and services provided, as well as the means of communication used to contact customers;

- Countries or territories of origin of the obligated entity's clients, or where they are domiciled or otherwise carry out their business;
- Countries or territories in which the obligated entity operates, directly or through third parties, whether or not they belong to the same group.

The review of the high risk level must be carried out at intervals of no more than 12 months, although it may be increased to 24 months when the nature, size and complexity of the activity pursued by the financial entity justifies it and the specific operating reality or business area in question presents a lower exposure to ML/TF risk.

The Bank will apply enhanced identification and due diligence measures whenever:

- occasional transactions, operations or any other form of relationship with natural and legal persons or similar, established in high-risk third countries;
- the establishment of the business relationship or the realisation of the occasional transaction takes place without the Client or their representative being physically present;
- Clients, their representatives or beneficial owners are Politically Exposed Persons;
- the Bank acts as a correspondent within the framework of correspondent relationships with third country respondents;
- identifies a situation of increased risk associated with a product, operation or distribution channel;
- identifies jurisdictions associated with a higher risk of ML/TF for certain business relationships or occasional transactions;
- in the case of cash deposits made by third parties into accounts held by Clients;
- provide services to *High Net Worth clients*;
- provides *trade finance* services.

As part of the enhanced identification and due diligence measures and, in particular, with regard to politically exposed persons, the Bank must:

- Adopt appropriate procedures to determine whether the Client may be considered a politically exposed person, and their actual residence situation, in the country or outside national territory.
- Adopt procedures for employees to obtain authorisation from the Compliance Department before establishing business relationships with such Clients;
- Take the necessary measures to determine the origin of the assets and funds involved in business relationships or occasional transactions;
- Carry out continuous monitoring and enhanced due diligence in business relationships with these

entities.

Examples of reinforced measures include

- Obtaining additional information on Clients, their representatives or Beneficial Owners, as well as on planned or realised transactions;
- Assessing their reputation;
- Previous activities carried out;
- The assessment of close family members and people recognised as being closely associated should refer to any Client, representative or beneficial owner, even if their status as a PEP or holder of other public or political office has not been identified;
- The carrying out of additional enquiries to verify the information obtained;
- The intervention of higher hierarchical levels within the Bank in order to authorise the establishment of business relationships and/or the execution of operations;
- The legitimacy of the funds involved in the business relationship or occasional transaction;
- The number, size and frequency of transactions estimated to be carried out within the scope of the business relationship;
- The intensification of the depth or frequency of the procedures for monitoring the business relationship;
- Reducing the time intervals for updating the information and other elements collected in the exercise of the duty of identification and diligence;
- The monitoring of the business relationship by the Regulatory Compliance Officer;
- The requirement to make the first payment for a given transaction via traceable means originating from a payment account opened by the Customer with an entity that, while not located in a high-risk third country, demonstrably applies identification and due diligence measures equivalent to those of the Bank;
- Consideration of means of proving the origin and legitimacy of the assets, namely:
    a) Income and, where applicable, wealth control statements;
    b) Reports of financial statements or legal certification of accounts;
    c) Pay slips;
    d) Certificates from public registers;
    e) Document proving the acquisition of inheritance;
    f) Public information, including from the media, provided it comes from an independent and credible source.

- The collection of information, in situations of increased risk, on the representative's or beneficial owner's relations with other jurisdictions, and associated persons that may influence their operations and, if they have their registered office or domicile in another jurisdiction, the reason why they intend to establish a business relationship or carry out an occasional transaction outside their jurisdiction;

- The consideration of adopting the following enhanced measures in situations where a situation of increased risk associated with a product, operation or distribution channel is identified:
    a) Limiting the number or amount of permitted transactions;
    b) Limiting use to certain jurisdictions;
    c) Limiting use to certain types of Customers;
    d) Limiting or restricting cash transactions;
    e) Requirement to carry out deposit, top-up, redemption or reimbursement operations through traceable means, namely through an account opened with a financial or other legally authorised entity which, not being located in a high-risk third country, demonstrably applies identification and diligence measures compatible with those provided for in the Law and in Banco de Portugal Notice no. 1/2022;
    f) Parameterisation of specific alerts in accordance with the risk attributed to the product, service or operation, defining and applying rules to adjust the risk of the product, service or operation when associated with high-risk customers.

- Adopting the following measures whenever the Bank identifies jurisdictions associated with a higher risk of ML/TF for certain business relationships or occasional transactions:
    a) Obtaining additional information on the jurisdiction in question, namely on the relevant regulatory framework and the existence of supervision;
    b) Intensifying the depth or frequency of monitoring procedures, particularly taking into account the origin and destination of transactions.

- The adoption of reinforced measures commensurate with the existing risks whenever the Bank provides services to High Net Worth customers, such as:
    a) Obtaining additional information when complying with complementary procedures;
    b) The intervention of higher hierarchical levels to: i) Authorise the establishment of the business relationship; ii) Approve the risk assessment associated with the business relationship and subsequent revisions;
    c) Reducing the time interval for updating information;
    d) Monitoring the follow-up of the business relationship;
    e) Reanalysing the risk and other elements associated with the business relationship to

which a higher degree of risk is attributed, on at least an annual basis.

- The adoption of at least the following reinforced measures proportional to the risk in the provision of *Trade Finance* services:
    a) Obtaining additional information on: i) Customers, their representatives and beneficial owners; ii) Planned or realised operations; iii) Counterparties to commercial transactions;
    b) The intervention of higher hierarchical levels to: i) Authorise the establishment of the business relationship; ii) Approve the risk assessment associated with the business relationship and subsequent revisions.

- Consideration of the following factors in situations of correspondence relationships considered to be high risk:
    a) The jurisdictions involved in the payment chain;
    b) The complexity of the payment chain and the clearing systems used between the entities authorised to practice financial services involved in that chain;
    c) The nature, size and number of those involved in the payment chain, as well as the jurisdictions in which they operate;
    d) The technology used to transmit information and process transactions in the payment chain;
    e) The volume and amount of transactions carried out or to be carried out.

4.9 Execution of the duty of identification and diligence by third parties

It is permitted to delegate the performance of identification and due diligence duties to a third party, with the exception of the duty to obtain information on the origin and destination of the funds handled, as well as the duty to maintain continuous monitoring of the business relationship, provided that this third party is an entity established in national territory or with headquarters in the European Union or an equivalent third country and that it is not high risk.

As part of its duty of identification and diligence, the Bank uses third parties to fulfil these duties.

To this end, the Bank ensures that third parties have the following characteristics:

a. they apply identification, due diligence and conservation procedures compatible with those provided for in Law 83/2017;

b. that they are subject to supervision compatible with the provisions of Chapter VII of Law 83/2017.

c. The third-party entity may not be established in high-risk third countries, with the exception of branches or subsidiaries majority-owned by obliged entities, or others of an equivalent nature, established in the European Union, if these branches or subsidiaries fully comply with the policies and procedures at group level.

d. In carrying out its duty of identification and due diligence by third parties, the Bank must also:

- Ensure that such entities are qualified to carry out the identification and due diligence procedures as its third parties;
- Assess, on the basis of information in the public domain, the reputation and suitability of the third parties;
- Complete the information gathered by the third parties or carry out a new identification, in the event of insufficient information or when the associated risk justifies it;
- Comply with all document conservation requirements as if they had carried out the identification and due diligence procedures carried out by third parties.

4.10. Own operations

In accordance with article 63 of Law 83/2017, the Bank is obliged to comply with preventive duties with regard to money laundering and terrorist financing in relation to operations it carries out:

a) On its own account;

b) On behalf of third parties who are not customers.

This concept includes transactions on own account or not, carried out between the Bank and any other entities that form part of the same group, outside the scope of a customer relationship.

Own-account transactions are those carried out in the name and on behalf of obliged financial entities, based on their own capital (own-account transactions), with a view to carrying out business or within the scope of contracts entered into.

In turn, transactions carried out in the Bank's own name on behalf of third parties who are not Customers correspond, for example, to transactions carried out by obliged entities when subcontracted to manage portfolios on behalf of others, in relation to portfolios under subcontracted management, whose owners are not its Customers (but those of the subcontracting entity), as well as intra-group transactions.

The Bank only carries out its own transactions on its own account, based on its own capital, and does not carry out (i) its own transactions on behalf of third parties (whether or not they are customers) (ii) its own intra-group transactions.

The Bank's own portfolio is not used for trading with clients.

The Bank's own operations are as follows:

(i) Pure own portfolio operations (securities, financial availability and shareholdings) in which the Bank takes on the role of selling or buying counterparty with clearing houses, *brokers*, selected

custodians and other entities;

(ii) Market Room operations contracted and carried out from a treasury management perspective.

The Compliance Department is responsible for monitoring the controls applicable to the execution of own operations under the terms and for the purposes of article 54 of Banco de Portugal Notice 1/2022.

4.11. Correspondent banks

A Correspondent Bank is a financial institution with which the Bank establishes a partnership agreement to represent it or be represented by it.

The Compliance Department is responsible for coordinating all actions and communications associated with PBC/CFT carried out within the scope of correspondent relationships.

Correspondent banking relationships carry a high risk of BC/FT for the Bank and, as such, additional procedures and controls must be put in place to mitigate them, namely:

a. Application of enhanced due diligence procedures which, among others, should include obtaining information on the nature of the correspondent bank's activity, its shareholders and Regulatory Compliance, as well as on the adequacy and effectiveness of its internal control system for AML/CFT and Sanctions;

b. Approval of the correspondent banking relationship by the Executive Committee, following an opinion from the Compliance Department;

c. Assessment, on the basis of publicly known information, of the correspondent bank's reputation and the characteristics of its supervision; and,

d. Application of reinforced monitoring measures on transactions.

In addition, all correspondent banking relationships are subject to specific, detailed written contracts.

The Bank takes the necessary measures in accordance with existing standards and good practices regarding the establishment or maintenance of relationships with Correspondent Banks.

4.12. Politically Exposed Persons

Under the terms of Law 83/2017, people in this category carry an increased risk of money laundering and terrorist financing, which justifies the implementation of special procedures for analysing and getting to know the client - enhanced due diligence. This issue will be discussed in a separate section below (see point 5).

4.13. Risk countries

Some countries can be classified as "Risk Countries" due to political unrest, armed conflicts, high levels of organised crime, recognised involvement in the production or trafficking of drugs, etc. Maintaining business relations with citizens of a Country at Risk, with people who are domiciled in that Country at Risk or who regularly conduct business with this type of country, may expose the Bank to greater risk.

The list of Risk Countries will be updated taking into account reports from governmental or international organisations in this field which divide risk countries into four Groups, Very High Risk Countries and High Risk Countries, Medium Risk Countries and Countries equivalent to Portugal, and whenever the Bank identifies jurisdictions associated with a higher risk of ML/TF.

4.14. High Risk Professions/Activities

This includes, among others, the designated non-financial activities and professions identified as higher risk and consequently subject to enhanced due diligence.

The Bank will not establish or maintain any relationship with Clients whose activities raise doubts as to their legality.

The Bank will seek references from all new Clients. References may be from a known Client, a Bank employee, the Bank's shareholders or companies belonging to the same corporate group. Client references do not exempt the Bank from carrying out full *due diligence* on the Client.

5. Politically Exposed Persons

The concept of PEP (as described in point 2. Concepts above) will be interpreted by the Compliance Department in accordance with the laws in force in Portugal and international best practices and understandings.

The Bank qualifies as a PEP those accounts in which any of its stakeholders identified in the account opening documents fall into this category.

If, in the course of their business relationship with the Bank, an account holder at a given time falls into the PEP category, the Compliance Department, upon becoming aware of this fact as part of its daily Customer filtering routines, must immediately update the KYC for the Customer.

The relationships that the Bank establishes with PEP Clients must be reviewed annually by the business area and the appropriate framework sent to the Compliance Department. If the political framework, the Client's position or the nature of the specific relationship with the Client changes considerably, the Client's file must be completely and comprehensively reassessed.

6. Control and conservation of documentation

The business areas are responsible for obtaining all the necessary documentation for opening an account, including the completed and signed forms. In cases where the account is analysed by the Compliance Department, it is the Compliance Department's responsibility to verify compliance with the requirements for opening an account and only in exceptional cases can it authorise the opening of an account in which a document is missing, ensuring that the account is blocked until the situation is resolved. If the Compliance Department refuses to open an account due to a lack of requirements, it will always provide summary reasons.

The Bank will keep all documentation collected for account opening and transactions on file for a period of 7 years.

The supporting documents for operations will be kept for a period of 10 years from the moment the orders are executed.

A register will be kept of the Bank's clients over the last 10 years.

7. Analysing and controlling operations

Any operation, regardless of its amount, which gives rise to suspicions of being related to money laundering or terrorist financing must be examined with particular attention.

If the analysis concludes that there are reasonable indications or certainties that the operation is related to money laundering or terrorist financing, the operation in question must be reported immediately to the competent authorities.

Customer transactions

The Bank analyses the operations carried out by its Customers in each segment on a daily basis, based on the Customer's level of risk and the characteristics of the operation. The Bank will adopt measures to determine each Client's profile when carrying out operations in order to identify deviating situations that should be analysed in greater detail.

The Compliance Department carries out checks prior to the execution of transactions, as well as *post-clearance* checks carried out after the transactions have been executed. Whenever necessary, the Compliance Department asks the business areas for additional information on each Client's activity with the Bank.

When the nature or volume of the Client's active or passive operations does not correspond to their

activity or operating history, the Compliance Department requests additional information from the business area regarding the origin and/or destination of the funds and the reasons for them.

When the nature or volume of the operation does not correspond to the Client's activity and the information on the origin / destination of funds referred to above is not considered complete and clear by the business area, it must report the occurrence and communicate the Client's operation to the Compliance Department.

The Bank will pay special attention to situations in which a large number of people have been credited with cash deposits to the same account without justification .

Whenever, as a result of exercising its duty of scrutiny, the Bank decides not to report the transaction to the competent authorities, it shall record it in a document or register:

a. The grounds for the decision not to report, including the reasons supporting the absence of concrete suspicion factors;

b. A reference to any informal contacts that may have been made with the Financial Intelligence Unit and the judicial and police authorities during the course of the examination, indicating the dates and means of communication used.

The conclusions of the analysis under the terms described above regarding the decision not to report a transaction must be kept for at least 7 years and be permanently available to auditors and supervisory and inspection bodies.

Transactions with correspondent banks

Transactions with correspondent banks always presuppose the establishment of a prior business relationship in which all the Identification and Due Diligence Duties set out in this policy are taken into account.

These operations are controlled by the Compliance Department on a filtering basis, using information extracted from the Bank's system, based on risk criteria established by the Compliance Department, identification of the parties involved in the operations, reasons and frequency of operations.

Trade Finance operations

The Compliance Department validates and verifies all operations related to *trade finance* activities, including letters of credit (including transferable ones) and documentary remittances.

8. Reporting suspicious transactions

Reporting

Any operation that may be considered suspicious because it shows signs of being related to the practice of money laundering or terrorist financing, as well as any subsequent circumstances related to these operations, must be reported immediately to the Compliance Department, which will act accordingly, namely with regard to compliance with the Duty to Report to the competent authorities.

The Bank must also report, on a systematic basis, to the PGR's DCIAP and to the FIU, any types of operations that are defined in the legislation in force.

The form, deadline, content and other terms of the systematic communications made by the Bank must comply with the legislation in force.

In addition, the Bank complies with the communication and reporting procedures set out in Law no. 97.

Reporting procedure

Any Bank employee who detects an operation suspected of money laundering or terrorist financing must report it immediately and simultaneously to the person in charge of their organisational unit and to the Compliance Department, which, after analysing the operation, will conclude whether or not to report it to the FIU and the PGR's DCIAP.

The internal reporting procedure must be particularly swift, in order to ensure compliance with the legal rules requiring immediate reporting of suspicious operations to the competent authorities.

Content of reports

Suspicious operation reports must contain the following information:

a. Identification of the natural or legal persons participating in the suspicious operation and the relationship between them;

b. A list of the transactions and the dates to which they relate, indicating their nature, the currency in which they are carried out, the amount, the place or places of execution, the purpose and the payment or collection instruments used;

c. Indication of the signs that lead to the suspicion that the operation may be related to money

laundering or terrorist financing.

Communication to DCIAP from the PGR and UIF and other competent authorities

Whenever a suspicion about an operation is brought to its attention, the Compliance Department must prioritise its analysis.

The report to the competent authorities of operations suspected of money laundering or terrorist financing will be made by the Compliance Department.

Reports of suspicious operations should be sent to the OPG and the FIU, via their own websites or by e-mail, at the following addresses:

Attorney General's Office: uai.dciap@pgr.pt

Financial Information Unit (UIF) of the Judicial Police: uif.comunicacoes@pj.pt

Any employee is free to report suspicious transactions to the authorities listed above.

Copies of all communications made under the duty to report must be kept for a period of 7 years from the moment the communication is made, as well as the respective proofs and dates.

With regard to facts related to the restrictive measures provided for in Law no. 97, the contact details of the respective competent authorities are also taken into account.

Exemption from liability

Under the terms of Law no. 83/2017, communications made in good faith do not constitute a breach of the duty of secrecy, nor do they imply the liability of the person making the communication.

Duty of confidentiality

The content of communications and the identity of the employee who first made the communication will be strictly confidential.

It is not permitted and constitutes a breach of legal duty to inform the Client or third parties, except for persons and bodies specially designated internally and the competent authorities, of the fact that an investigation is underway into an operation for its possible link to money laundering or terrorist financing.

Failure to comply with the duty of secrecy constitutes an administrative offence punishable by a fine of €50,000.00 to €5,000,000.00 if the perpetrator is a legal person, or a fine of €25,000.00 to €5,000,000.00 if the perpetrator is a private individual.

Revealing or favouring the discovery of the identity of someone who provided information that led to the investigation of a particular operation is punishable by up to 3 years in prison or a fine.

9. Monitoring branches and subsidiaries

In the light of the principles of proportionality and appropriateness, the policies and other internal regulations applicable to the Bank in terms of PBC/CFT are extended to branches and subsidiaries, and the action and diligence parameters of the Compliance function are applied, under the terms and for the purposes of article 22 of Law no. 83/2017,

APPROVAL, COMMUNICATION AND REVIEW

1. Approval and communication

This Policy is approved by the Board of Directors or the Executive Committee and comes into force on the day following its approval.

This Policy will be communicated to all employees via the Intranet.

2. Review

This Policy will be reviewed annually or whenever the Executive Committee or the Board of Directors deems it necessary, in order to ensure compliance with the legal and regulatory rules to which the Bank is subject.

Changes to this Policy are subject to approval by the Board of Directors