HAITONG

REGULATION No. COM05.R05

Anti-Money Laundering and Countering the Financing of Terrorism Regulation of Haitong Bank S.A

Approved by the Board of Directors
on 11/11/2026

TABLE OF CONTENTS

1. OBJECTIVE 4
2. LEGAL FRAMEWORK 4
3. RECIPIENTS 7
4. RESPONSIBILITY 7
5. DEFINITIONS 8
6. GOVERNANCE FRAMEWORK 13
6.1. ALL EMPLOYEES OF THE BANK 13
6.2. MANAGEMENT BODY 14
6.3. COMPLIANCE DEPARTMENT 15
6.4. INTERNAL AUDIT DEPARTMENT 16
6.5. HUMAN RESOURCES DEPARTMENT 16
7. PREVENTIVE DUTIES OF AML/CFT 17
7.1. DUTY TO CONTROL 17
7.2. DUTY TO IDENTIFY AND APPLY DUE DILIGENCE MEASURES 18
7.3. DUTY TO REPORT SUSPICIOUS TRANSACTIONS 18
7.4. DUTY TO REFRAIN 19
7.5. DUTY TO REFUSE 19
7.6. DUTY TO KEEP DOCUMENTS AND RECORDS 19
7.7. DUTY OF SCRUTINY 20
7.8. DUTY TO COOPERATE 21
7.9. DUTY OF NON-DISCLOSURE 21
7.10. DUTY TO PROVIDE TRAINING 21
8. AML/CFT GLOBAL RISK MANAGEMENT MODEL 21
8.1. RISK MANAGEMENT 22
8.2. EFFECTIVENESS ASSESSMENT 23
8.3. CLIENTS ML/FT RISK SCORING 24
8.4 INFORMATION SYSTEMS 24
8.5. WHISTLEBLOWING SYSTEM 24
8.6. MONITORING OF BRANCHES AND AFFILIATES 25
8.7. INDEPENDENT TESTING 25
9. CLIENT ONBOARDING 25
10. KNOW YOUR CLIENT 29
10.1. SIMPLIFIED MEASURES 32
10.2. ENHANCED DUE DILIGENCE MEASURES 33
10.3. POLITICALLY EXPOSED PERSONS 34
10.4. ADDITIONAL DUE DILIGENCE 35
10.5. PERFORMANCE BY THIRD PARTIES OF THE DUTY TO IDENTIFY AND DUE DILIGENCE 35
11. ARCHIVE 36
12. DISCLOSURE 36
13. CONTROL OF VERSIONS 36
SCHEDULE I - ILLUSTRATIVE LIST OF FACTORS AND TYPES INDICATING A POTENTIALLY LOWER RISK 39
SCHEDULE II - ILLUSTRATIVE LIST OF FACTORS AND TYPES INDICATING A POTENTIALLY HIGHER RISK 41
SCHEDULE III - ILLUSTRATIVE LIST OF POTENTIAL SUSPICION INDICATORS 44

14. ANNEX I 53
AML/CFT RISK ASSESSMENT METHODOLOGY OF HAITONG BANK S.A. 53
I. CURRENT AML RISK MODEL 53
II. RISK ASSESSMENT METHODOLOGY 54
III. KEY INPUTS FOR THE RISK ASSESSMENT 55
IV. CLASSIFICATION OF CLIENTS IN TERMS OF AML/CFT RISK 55
V. AML/CFT RISK ASSESSMENT CATEGORIES 55
VI. AML/CFT RISK ASSESSMENT FACTORS 56
VII. MITIGATING FACTORS 59
VIII. OUTPUTS OF THE RISK ASSESSMENT 59
IX. PROBABILITY AND IMPACT OF RISK FACTORS 60
X. PERIODIC REVIEW AND UPDATE OF AML/CFT RISK ASSESSMENT 61

1. OBJECTIVE

The objective of this Regulation is to determine, at the level of internal regulations, the essential elements to be observed in the context of prevention, detection and fight against money laundering, terrorist financing, financing of the proliferation of weapons of mass destruction, as well as for effective compliance with the current regime of sanctions and restrictive measures.

Moreover, in the context of anti-money laundering and countering the financing of terrorism (hereinafter "**AML/CFT**") rules, this Regulation also aims at addressing the rules regarding the governance model and the responsibilities of the relevant stakeholders for the purposes of client acceptance at Haitong Bank, S.A. (hereinafter "**Bank**"). Specially, this Regulation will lay down the set of criteria and categories that should guide the whole Bank in the context of acceptance or refusal of new clients and establishment of any business relationships with new counterparties or any other entities.

2. LEGAL FRAMEWORK

This Regulation is drawn up pursuant to the provisions of the regulatory acts that directly or indirectly govern the fight against money laundering and terrorist financing (AML/CFT) framework.

- Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019, laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences.
- Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 - on combating money laundering by criminal law.
- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 - amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Directive (EU) 2016/2258 of the European Parliament and of the Council of 06 of December 2016 regarding access to anti-money-laundering information by tax authorities.
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 - on controls on cash entering or leaving the Union.
- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds.
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical

standards for the minimum action and the type of additional measures that credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries.

- Commission Delegated Regulation (EU) 2018/1108 of 7 May 2018 - supplementing Directive (EU) 2015/849 with regulatory technical standards on the criteria for the appointment of central contact points for electronic money issuers and payment service providers and with rules on their functions.
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 - supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies.
- Law No 58/2020 of 31 August 2020 - transposes Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, amending various laws (Portuguese only).
- Law No 97/2017 of 23 August 2017 - Regulates the implementation and enforcement of restrictive measures adopted by the United Nations or the European Union and establishes the penalties applicable to infringements of these measures.
- Law No 92/2017 of 22 August 2017 - Requires the use of a specific means of payment in transactions involving amounts equal to or greater than EUR 3000 (in Portuguese only).
- Law No 89/2017 of 21 August 2017 - Approves the Legal Regime of the Central Register of Beneficial Ownership, provided for in article 34 of Law no. 83/2017, of August 18 (in Portuguese only).
- Law No 83/2017 of 18 August 2017 - Establishes measures to combat money laundering and terrorism financing, partially transposing the Directives 2015/849/EU of the European Parliament and of the Council of May 20, 2015, and 2016/2258/EU of the Council of 6 of December 2016.
- Law No 52/2003 of 22 August 2003 – Sets forth measures to combat terrorism.
- Law No 5/2002 of 11 January 2002 – Lays down measures to combat organized crime and economic and financial crime and provides for a special system for the collection of evidence, the violation of professional secrecy and loss of assets to the State in relation to unlawful acts of a specified type, such as money laundering and terrorist financing (in Portuguese only).
- Decree-Law No 91/2018 of 12 November 2018 - Approves the Legal Framework for Payment Services and Electronic Money.

- Decree-Law No 61/2007 of 14 March 2007 – Approves the legal system governing the control of cash carried by natural persons entering or leaving the EU through the Portuguese territory, and the control of cash movements with other EU Member States.
- Decree-Law No 298/92 of 31 December 1992 – Approves the Legal Framework of Credit Institutions and Financial Companies.
- Ministerial Order No 310/2018 of 4 December 2018 - Regulates article 45 of Law 83/2017, defining the types of operations to be reported by obliged entities to the UIF (the Portuguese police's financial information unit) and the DCIAP (the central investigation department of Portugal's public prosecution service).
- Ministerial Order No 345-A/2016 of 30 December 2016 – Establishes the list of countries, territories and regions with privileged taxation systems.
- Ministerial Order No 150/2004 of 13 February 2004 - Approves the list of countries, territories or regions with privileged and more favorable taxation.
- Portuguese Penal Code (whose Article 368-A typifies the laundering crime).
- Notice of Bank of Portugal No 1/2022 of 6 June 2022 - Governs enforcement conditions, procedures, instruments, mechanisms, enforcement measures, reporting obligations and other aspects necessary for ensuring compliance with obligations for the prevention of money laundering and terrorist financing, within the activities of financial entities subject to the Bank's supervision, as well as the means and mechanisms necessary for such entities to comply with the duties enshrined in Law No 97/2017, and also the measures that payment service providers must adopt to detect transfers of funds with missing or incomplete information on the payer or payee.
- Notice of Bank of Portugal No. 3/2021, of 13 April 2021, regulating the registration process with the Bank of Portugal of entities that intend to carry out, within Portuguese territory, activities with virtual assets subject to registration, as well as subsequent changes to the elements to be registered.
- Notice of Bank of Portugal No 3/2020, of 15 July 2020 - Regulates the systems of governance and internal control and defines the minimum standards on which the organizational culture of the entities subject to supervision by Bank of Portugal must be based.
- Notice of Bank of Portugal No 8/2016 of 30 September 2016 - Establishes the duties of registration and communication to the Bank of Portugal of payment operations, corresponding to payment services, whose beneficial owner is a natural or legal person having its head office in an offshore jurisdiction.

- Notice of Bank of Portugal No 7/2009 of 16 September 2009 – Prohibits credit granting to entities having their head office in an offshore jurisdiction considered as non-cooperative or whose ultimate beneficiary is unknown.
- Instruction of Bank of Portugal No 25/2020 of 24 September 2020 - Report on the activity carried out in Portuguese territory by financial entities with their head office in another Member State of the European Union, operating in Portugal under the freedom to provide services.
- Instruction do Bank of Portugal n.º 8/2024 - Sets forth the requirements for entities subject to the Bank's supervision to regularly report information to Bank of Portugal in the field of prevention of money laundering and terrorist financing.
- Portuguese Securities Market Commission Regulation No. 02/2020, of 17th March 2020, regarding the Prevention of Money Laundering and the Financing of Terrorism.

3. RECIPIENTS

a) The content of this Regulation represents a minimum standard that shall apply to the Bank and its subsidiaries and branches (“Haitong Bank”).
b) In case of conflict between any provision of this Regulation and the local laws and regulations applicable to any Bank's branch or representative office, the relevant local laws and regulations shall prevail.

The standards laid down in this document must be complied with by the members of the corporate bodies and employees of the Bank.
The Bank must ensure that the AML/CFT principles and procedures that apply internally are extended to all its branches and affiliates, to the extent possible, specifically:

i. to assess the risks inherent in the business carried out;
ii. to exchange information within the Bank with a view to achieving the goals sought by the AML/CFT regulation.

If the legislation of the country of incorporation of any branch or affiliate prevents application of the principles, policies or measures set forth in this document, the Bank must inform the Bank of Portugal thereof and of the policies adopted to address the increased risk resulting therefrom.

4. RESPONSIBILITY

a. This Regulation is sponsored by the Compliance Department.
b. This Regulation is reviewed at least once a year or whenever any amendment thereto becomes necessary.

c. The Internal Audit Department and external auditors shall also complete efficiency and adequacy tests on the existing controls and procedures of the Bank.

5. DEFINITIONS

Adverse Media – also known as negative news is defined as any kind of unfavorable information (derived from predefined lists or keywords) and can be found across a wide variety of sources including web posts, blogs and social feeds- not only more "traditional" news outlet such as newspapers in print or online or broadcast news across radio and TV;

Account – bank account opened to create one of the deposit methods provided for in article 1 of Decree-Law no. 430/91, of 2 November, as well as any other payment account within the meaning of paragraph g) of article 2 of the Legal Regime for Payment Services and Electronic Currency (Decree-Law no. 91/2018 of 12 November); the Haitong bank account is a payment account that allows the transfer of deposited funds at any time, and it is necessary for the contracting of other banking services, such as the conclusion of a credit agreement or a term-deposit;

Assets – anything of value owned by a person or business and can be movable or immovable, tangible, or intangible. This includes legal documents in any form (including electronically or digitally) evidencing ownership of or other rights to such Assets;

Bearer – bearer instruments, which include Bearer shares, Bearer bonds and Bearer stock, are documents that give the holder of the document rights of ownership or title to the underlying property, such as shares or bonds. Bearer instruments differ from normal registered instruments in that no record is kept of who owns the underlying property, or of the transactions involving transfer of ownership;

Beneficial Owner:

a) the natural person(s) who ultimately own or control a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity;
b) the natural person(s) who otherwise control the legal entity;
c) the natural person(s) who hold the position of senior managing officials if, after having exhausted all possible means and provided there are no grounds for suspicion.

Business Relationship - any relationship of a business, professional or commercial nature, including those established within the scope of an investment or divestment operation, which, at the time of establishment, is or is expected to be long-lasting, stable, and continuous over time, regardless of the number of individual operations that integrate or will integrate the established relational framework;

Business Restrictions – permanent or temporary requirements or conditions on client relationship such as limits on transactions, accounts, and products;

Breach – an act or failure to act which contravenes the requirements of applicable obligations of the Regulation;

Client Due Diligence (CDD) – identification and verification procedure that ensures the collection and evaluation of relevant information about a Client/Counterparty, to identify the level of risk associated with establishing a business relationship with it;

Client - natural, legal person (of a corporate or non-corporate nature), or center of collective interests without legal personality, who comes into contact with the Bank for the purpose of providing a service or making available a product, through the establishment of a business relationship or the execution of an occasional transaction; For the purpose of the KYC procedures, the Bank considers Clients, natural or legal person with a bank account associated to the services provided by the Bank and the KYC rules applied are the ones defined on the PM254 - Account Opening Procedures, and

Counterparty is a legal person which the business relationship and the services provided by the Bank does not oblige to have a bank account associated. For those, the KYC rules that must be applied are the ones defined at the PM019 - Counterparty Identification Procedures.

Country Risk – the country risk derives from the client's citizenship, country of domicile, place of incorporation, place of principal activities or operations, and origin and destiny of funds. It considers various indicators connected to Money Laundering, Terrorist Financing, Sanctions, Proliferation Financing, Bribery and Corruption, Tax Evasion offences and other Financial Crime;

Correspondent Relationship – a correspondent relationship exists where Bank provides either:

- specific Banking Services related to the execution of payments including the maintenance of a current or payments account and the provision of related services (such as cash management, international funds transfers, cheque clearing and foreign exchange services) to credit institutions (and other institutions in third countries that carry out equivalent activities); or
- other services to credit and financial institutions (and other institutions in a third country that carry out equivalent activities) that support the provision of Banking and financial services such as the carrying out of security transactions or funds transfers.

Employee – natural person who, in the name or interest of the Bank and under its authority or in its dependency, participates in the execution of any operations, acts or procedures specific to the activity pursued by the Bank, regardless of the nature of the underlying link;

Enhanced Due Diligence (EDD) – procedure that involves the application of an elevated level of Due Diligence measures applicable to client relationship bearing a high level of AML/CFT, including PEP's, holders of other political or public positions (TOCPP's) or their correspondence relationships, in operations or occasional transactions carried out by them;

Gambling Entities – any entity offering services which involve wagering a stake with monetary value in a game of chance, including lotteries and those with an element of skill such as casino games, poker games and betting transactions that are provided at a physical location or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services;

High-risk third countries – non-European Union countries or jurisdictions identified by the European Commission as having national ML/FT regimes with strategic deficiencies considered to pose a significant threat to the European Union financial system;

Jurisdictions associated with a higher ML/FT risk - jurisdictions that, based on a prior assessment, whether they are considered to present a higher risk of ML/FT, including, but not limited to, high-risk third countries;

Know Your Client (KYC) – the process of conducting Due Diligence on the Client/Counterparty and recording the respective information and documents in client management information system, SAP-MER; this process should guarantee knowledge by the Bank of the Clients and Counterparties with whom it interacts relate, namely through the application of Customer Due Diligence activities, acting in a preventive and/or reactive manner based on the risk and the verification of occurrences of ML/FT and Restrictive Measures;

Know Your Transaction (KYT) – knowledge and constant monitoring by the Bank of the profile transactions of its Clients and Counterparties, carrying out the assessment based on the risk-based approach in force throughout the moment and knowledge resulting from KYC, the underlying economic rationale, and the potential ML/FT risk and Measures Restrictive;

Money Laundering - pursuant to the definition adopted by the Bank of Portugal[1], "money laundering is the process through which the authors of criminal activities conceal the true source of the property and revenue (benefits) obtained by illicit means, transforming the liquidity from such activities into legally reusable money, by disguising the origin and true owner of the funds". Law no. 83/2017 expands this concept, stating that money laundering also includes the acquisition, ownership or use of property, knowing, at the time of its receipt, that such property is derived from criminal activity or from an act of participation in such activity, as well as the participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of these actions. In addition, it is the process by which one intends to conceal the origin of assets and income (advantages) obtained from illicitly, transforming the liquidity resulting from these activities into legally reusable capital, disguising the origin or true beneficiary of the funds. Money laundering can encompass three phases: placing assets

[1] https://www.bportugal.pt/en/page/branqueamento-de-capitais-e-financiamento-do-terrorismo

and income in financial and non-financial circuits; circulation subjecting assets and income to multiple and repeated operations; and integration through which assets and income, already recycled, are reintroduced into legitimate economic circuits;

Occasional transaction - any transaction that is carried out by the Bank outside the scope of a business relationship already established, characterized, in particular, by its expected punctuality. This includes operations of change and waste carried out on a non-continuous and punctual basis, to Clients with whom the Bank does not have a commercial relationship established;

Politically Exposed Person (PEP) – any individual who is or has been entrusted in the immediately preceding year with any Prominent political or public function[2], as well as his/her immediate family members (spouse / partner; as well as parents, stepparents, parents-in-law, children, stepchildren, and children-in-law) and close business associates.

Pooled Account – Bank account opened by a client to hold funds from its clients, who have no powers for operating the Account and, therefore, they will not be able to give direct instructions to the Bank to carry out transactions;

Relevant Employee – employee (internal or external) of the Bank who:

i) is a member of the Management Body;

ii) performs functions that involve direct contact, in person or remotely, with Bank Clients;

iii) exercise functions within the Bank that are related to compliance with the regulatory framework in matters of AML/CFT; or

iv) be classified as such by the Bank;

Restrictive Measures - multilateral instrument, of a political-diplomatic nature, of a non-punitive nature, which aims to change actions or policies, such as violations of international law or human rights, policies that do not respect the rule of law or democratic principles, and may be addressed to governments of third countries, non-state bodies (groups or organizations) and natural and legal persons.

A restrictive measure is a temporary restriction on the exercise of a particular right, through the imposition of a prohibition or an obligation.

Law No. 97/2017, of 23 August, regulates the application and enforcement of restrictive measures approved by the United Nations or the European Union and establishes the sanctioning regime applicable to the violation of these measures.

The Direção-Geral de Política Externa do Ministério dos Negócios Estrangeiros and the Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais do Ministério das Finanças jointly carry out the tasks of national competent authorities for restrictive measures.

[2] Article 2/1/cc) of Law No. 83/2017.

Among the restrictive measures applicable, the freezing of funds and economic resources deserves to be highlighted.

The freezing of funds is an action aimed at preventing the movement, transfer, alteration, use or operation of, or access to, funds which are likely to cause a change in their value, volume, location, ownership, possession, nature, destination, or any other change that may allow their use, including the management of securities portfolios.

The freezing of economic resources is an action aimed at preventing the movement, transfer, disposal, or encumbrance of assets of any kind, tangible or intangible, movable, or immovable, which are not funds but which can be used to obtain funds, goods or services, by any means, including through their sale, lease or mortgage.

Shell Bank – means any entity engaged in its own activity or equivalent to that of a financial entity that:

I. Is constituted in a country or jurisdiction in which does not have a physical presence that involves an effective direction and management, not confining physical presence to the mere existence of a local agent or subordinate employees; and

II. does not form part of a regulated financial Bank.

Source of Funds – the source of funds involved in the business relationship or occasional transaction, including the activity that generated, and the means used to transfer them;

Source of Wealth – refers to the underlying economic, business, or commercial activities that generate or contribute to the Client overall wealth;

Senior Top management – any Employee with sufficient knowledge of the exposure of the Bank to the AML/CFT risk and who performs executive functions that allow to take decisions that directly affect the respective exposure, not necessarily being a member of the management body;

Terrorist Financing – the conduct foreseen and punished by article 5.º-A of Law no. 52/2003, of August 22, regarding the supply, collection or holding (directly or indirectly) of funds or assets of any nature, as well as of products or rights capable of being transformed into funds, intended for use (total or partial) in planning, preparation, or commission of terrorist acts. In terrorist financing, one of the financiers' primary purposes is to hide the purpose for which the funds are intended, one of the biggest difficulties being the fact that, frequently, the amounts involved are relatively low and usually of legal origin (e.g., donations to charities or non-profit organizations), making it more difficult to detect the operations in question;

Transfer of Funds - any transfer within the meaning of paragraph 9 of article 3 of Regulation (EU) 2015/847.

Waiver – the collective term for an exception from, modification or dispensation to AML/CFT Regulation or procedure requirements;

6. GOVERNANCE FRAMEWORK

Preventing, detecting, and combating ML/FT, as well as Sanctions and Restrictive Measures requires the definition of a specific governance model that allows the identification, monitoring and control of the Bank ML/FT risks and Sanctions/Restrictive Measures, ensuring functional segregation between the competencies and responsibilities of the Bodies involved.

Therefore, and to comply with the principle mentioned above, the Bank operationalizes the governance of ML/FT risk and Sanctions/Restrictive Measures with the establishment of 3 lines of defense and ensuring throughout this Regulation the definition of their respective powers and responsibilities.

The governance model adopted by the Bank in this matter ensures strict distinction between the business and support bodies, the management and control bodies and the evaluation or independent review.

6.1. All employees of the Bank

In the context of AML/CFT, the Bank and its Employees are legally bound to a number of duties, namely:

- duty to control, by determining and ensuring the application of appropriate internal policies and procedures for the effective management of any risks of money laundering and compliance with the legal and regulatory provisions;
- duty to identify and apply due diligence measures to Clients, Counterparties and their representatives and beneficial owners;
- duty to report suspicious transactions to the Compliance Department
- duty to refrain from executing suspicious transactions, followed by a report to the DCIAP and the FIU and subject to confirmation by these authorities;
- duty to refuse to establish business relationships, carry out occasional transactions or carry out other transactions when the client does not supply his/her/its identification details or those of the person on whose behalf he/she/it is acting or information on the nature, subject matter and purpose of the business relationship;
- duty to retain the relevant documentation for seven years;
- duty to examine certain behaviors, activities or transactions which might correspond to a money laundering offence;
- duty to cooperate with the competent authorities, supplying any information requested;

- duty of non-disclosure, which prohibits the Bank's Employees from disclosing to the Client or any third-party that he/she/it is being investigated in this context or that a suspicious transaction report has been made[3];
- duty to train Employees, so as to permit the identification of any transaction which might be related to money laundering, as well as the performance of the other duties, as a means to prevent this sort of transactions.

6.2. Management body

Pursuant to article 13 of Law no. 83/2017, the management body is responsible for:

- appointing a member of the management body to be responsible for complying with the provisions of Law no. 83/2017, Notice of the Bank of Portugal no. 1/2022 and other applicable regulations;
- approving AML/CFT policies, procedures, and controls;
- possessing adequate knowledge of the main risks of money laundering and terrorist financing to which the Bank is exposed, as well as of the processes used to identify, assess, monitor, and control these risks[4];
- ensuring an appropriate AML/CFT organizational structure, preventing conflicts of interest;
- fostering an AML/CFT institutional culture supported by high standards of ethics and integrity;
- appointing a money laundering reporting officer (“MLRO”);
- periodically assessing the effectiveness of the policies and controls, ensuring that any shortfalls detected are corrected.

In accordance with no. 3 of the article, the management body must refrain from interfering with any exercise of the duty to report suspicious transactions, which shall exclusively be exercised by the MLRO.

Notwithstanding, under the terms of article 4 no. 1-g) of the Notice no. 1/2022, the appointed member of the management body is responsible for reviewing any decision to refrain from exercising the duty to report made by the MLRO, whenever he/she concludes there are no potential suspicions.

The management body must ensure that the MLRO:

- exercises his/her duties in an independent, ongoing, and effective manner and with the required autonomy to make decisions;

[3] Breach of this rule is a criminal offence, punishable under article 157 of Law no. 83/2017 by imprisonment for up to three years or fine.
[4] In accordance with the Bank's AML/CFT risk assessment methodology.

- has the appropriate repute, professional qualifications, and availability for this function;
- has appropriate technical, material, and human means and resources, including any employees necessary for the proper performance of his/her function;
- has unrestricted access in a timely manner to any internal information material for exercising his/her function, in particular information on compliance with the duty to identify and apply due diligence measures and records of transactions made;
- is not subject to any potential conflict of functions, in particular when his/her duties are not segregated.

6.3. Compliance Department

Compliance is the Department in the Bank which act as the 2LoD Risk Control Function for the Money Laundering, Sanctions and Embargos risk types.
Article 16 of Law no. 83/2017 and article 5 of Notice no. 1/2022 of the Bank of Portugal require the Bank to appoint a money laundering reporting officer (MLRO), who must be a member of its senior management or an equivalent officer and who shall have exclusive responsibility for the actual application of policies, procedures and controls appropriate to an effective management of ML/FT risks and controlling compliance with the applicable legal and regulatory provisions.

Pursuant to the aforementioned articles, the MLRO shall be responsible for:

- taking part in the drawing up of and issuing a prior opinion on any AML/CFT policies, procedures, and controls;
- monitoring, on an ongoing basis, the adequacy, sufficiency, and update of AML/CFT policies, procedures and controls, proposing any necessary amendment thereto;
- participating in the establishment, monitoring and assessment of the internal training policy;
- ensuring that all material information from the various business areas is centralized;
- acting as a point of contact for judiciary, police, and supervisory and inspection authorities, notably by complying with the duty to report and ensuring compliance with other reporting and cooperation obligations;
- ensuring the sufficiency, accessibility, and comprehensiveness of information on the internal control system and of the policies and instrumental procedures and controls for its application made available to the relevant employees of the financial institution;
- supporting the preparation and execution of periodic assessments of the adequacy of AML/CFT policies, procedures, and controls;

- proposing the adoption of any corrective action which might prove necessary to the management body;
- coordinating the drawing up of notices, reports, and other information to be sent to the management body and relevant external entities;
- ensure the immediate availability to all relevant Employees of Bank of Portugal's communications made under the Law, the Notice or other regulatory documents;
- duty to report suspicious transactions to the Central Department for Investigation and Penal Action (Departamento Central de Investigação e Ação Penal do Ministério Público - DCIAP) and to the Financial Information Unit (FIU) of the Criminal Police;
- on the matters related to restricted measures, duty to communicate, if applicable, to Direção-Geral de Política Externa do Ministério dos Negócios Estrangeiros and to Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais do Ministério das Finanças

Compliance Department participates in the Bank's functional committees, in particular the Credit Committee, the Investment Banking Global Adoption Committee, and the New Business Committee, by issuing a mandatory previous opinion on all proposals.

6.4. Internal Audit Department

The audit department is specifically responsible for:

a) Monitor, as a 3rd line of defense body, the performance of the Bank's various functional areas, including the Compliance Department, by periodically carrying out effectiveness tests on the AML/CFT Control Systems implemented by the Bank, as defined in the audit plan;

b) Report the results of audits carried out, communicating the respective results;

c) Develop continuous monitoring of deficiencies identified in this context.

6.5. Human Resources Department

The Human Resources department is specifically responsible for:

a) Ensure attendance at training with the design and implementation of annual training plans within the scope of AML/CFT, previously approved by Compliance;

b) Whenever applicable, ensure the evaluation of Employees covered by the training duty within the scope of AML/CFT, in accordance with the training programs provided for in this Regulation;

c) Ensure the record of internal or external training actions carried out.

7. Preventive Duties of AML/CFT

Compliance with laws and regulations that are intended to combat and prevent money laundering and terrorist financing should be a priority of the financial institutions.

In order to ensure full compliance with applicable laws and regulations, financial institutions and their employees shall observe the following preventive duties:

7.1. Duty to control

The Bank, through the Compliance Department, must determine and apply internal policies, procedures and controls appropriate to effectively manage the risks of money laundering and to comply with the legal and regulatory provisions in this respect. The policies, procedures and controls determined by the Bank must include, at least:

- the establishment of an effective risk management model, with practices appropriate for the identification, assessment, and mitigation of any risks of money laundering to which the Bank is, or might become exposed;
- the development of client onboarding policies, procedures and controls;
- establishment of appropriate staff ongoing training programs, applicable from admission;
- appointment of a MLRO;
- establishment of formal systems and processes to capture, process and store information that support, in a timely manner:
  i. the analysis and decision-making process, in particular with regard to the monitoring of clients and transactions and examination of potential suspicions;
  ii. compliance with the duties to report and to cooperate;
  iii. establishment of safe channels making it possible to ensure full confidentiality of any requests for information;
- communication to staff of duly updated and accessible information on the respective AML/CFT internal standards;
- establishment of mechanisms to control the conduct of the Bank's employees;
- establishment of appropriate tools or IT systems, as required for the effective management of the risks of money laundering;
- establishment of mechanisms making it possible to periodically test their quality, adequacy and effectiveness, including, if applicable, an independent audit function;
- establishment of appropriate internal resources enabling the Bank's employees to report any breach of this Regulation through a specific, independent and anonymous channel;
- development of personal data protection policies and procedures.

All AML/CFT policies, procedures and controls must be documented and the Bank, through the Compliance Department, must review them to ensure that they remain up to date.

7.2. Duty to identify and apply due diligence measures

The duty to require identification falls under the KYC – Know Your Client – and KYB - Know Your Business – practices and applies to all Clients and Counterparties before beginning to execute any transaction.

By means of internal regulations, the Bank lays down the rules regulating the collection of all identification details of its Clients and Counterparties, as well as the respective evidence required, in accordance with Law no. 83/2017 and Notice no. 1/2022 of the Bank of Portugal.
This duty must be performed whenever:

a. a business relationship is established, or an occasional transaction is carried out and:
   i) any bank account is opened;
   ii) the Bank, without opening an account, executes any transaction, even if only occasional, whose amount in isolation or in aggregate (several transactions apparently related to one another) is equal to or greater than €15,000 or corresponds to any transfer of funds in excess of €1,000;
b. there is a suspicion that the transactions might be related to money laundering or terrorist financing, regardless of the amount or any exemption or threshold;
c. there are doubts about the veracity or adequacy of previously obtained client identification data.

7.3. Duty to report suspicious transactions

The Bank, through the MLRO, shall immediately inform the DCIAP and the FIU whenever it knows, suspects, or has reasonable grounds to suspect that any cash or other property, regardless of the amount or value involved, is proceeds of criminal activity or is related to terrorist financing.

Accordingly, the Bank's employees must advise the Compliance Department whenever they have reason to suspect that they are facing a situation with these characteristics.

In such cases, the Bank’s employees must not contact the Client for further clarifications, without prior guidance from Compliance, nor disclose the existence of the internal report to the Client or any unauthorised person.

7.4. Duty to refrain

Under the duty to refrain, it is prohibited to execute any transaction which the Bank suspects of being related to any money laundering offence. In the event of such a suspicion, the MLRO must report to the DCIAP and the FIU that the Bank has refrained from executing a transaction or set of transactions. Following this notice, the DCIAP may, within seven business days, order the temporary suspension of the respective execution, which will subsequently be subject to confirmation by the court in the context of a criminal enquiry.

The Bank may execute transactions with regard to which it has complied with its duty to refrain, under the following circumstances:

a. when it is not notified, within seven business days of the aforementioned report, of the decision to order a temporary suspension;
b. when it is notified, by the deadline referred to in the preceding paragraph, of the DCIAP's decision not to order a temporary suspension, in which case transactions may be immediately executed.

7.5. Duty to refuse

The heads of the Bank's business areas must refuse to execute transactions when the Client does not supply: (i) his/her/its identification or the identification of the person on whose behalf he/she/it is effectively acting, in the terms set forth in the law; (ii) information on the beneficial owner and the ownership and control structure; (iii) information on the nature and purpose of the business relationship and the origin of the funds.

In this event, the Compliance Department will analyze the underlying circumstances and, if it suspects that the situation might be related to any money laundering offence, it will make the notifications foreseen in the duty to report and consider terminating the business relationship.

If a decision to terminate the relationship is taken, the Bank shall inhibit any transactions involving funds of the client and contact the client to transfer the funds for an account held by him/her/it in another financial institution.

7.6. Duty to keep documents and records

All the documentation collected and generated in the context of the money laundering and terrorist financing system must be retained for a seven-year period.

This set of information includes: the policies, procedures and controls, as well as the periodic assessments of their effectiveness; the risk assessments performed in accordance with the approved methodology; documents evidencing compliance with the duty to identify and to apply due diligence measures (in this case, the Bank must retain the documentation for seven years after the end of the business relationship with the client); reports of shortcomings made internally by the Bank's employees (whistleblowing); suspicious transaction reports submitted to the FIU and the DCIAP, as well as systematic transaction reports; the analyses and findings made in the context of exercise of the duties to refrain, to refuse and to examine; records of training actions.

Originals, copies, references or any other durable media, with an identical value as evidence, of supporting documents and transaction records must always be retained, so as to make it possible to recreate the transaction, for at least seven years after its execution, even if, should it fall within a business relationship, such business relationship has already ended.

7.7. Duty of scrutiny

All the Bank's employees must analyze with particular care any behavior, activity, or transaction whose characteristics make it particularly liable to be related to money laundering, in particular:

a. the nature, purpose, frequency, complexity, unusualness, and exceptionalness of the behavior, activity or transaction;
b. the apparent absence of an economic purpose or a lawful end associated with the behavior, activity or transaction;
c. the amounts, origin and destination of the funds moved;
d. the place of origin and destination of the transaction;
e. the means of payment used;
f. the nature, activity, patterns of operation and the parties' economic condition and profile;
g. any other risk features identified in the transaction;
h. the type of transaction, product, shareholding, or legal arrangement structure that might favor anonymity.

The outcome of this analysis must be written down and retained for at least seven years, being open to inspection by auditors and supervisory and inspection entities.

7.8. Duty to cooperate

The Bank, through the Compliance Department, particularly the MLRO, must provide any assistance requested by Public Attorney's Office (DCIAP) and police (FIU), supervisory and tax and customs authorities in the context of the duty to cooperate, notably by supplying all information and submitting all documents requested by the aforementioned authorities.

7.9. Duty of non-disclosure

The Bank, through the members of its bodies, its employees and any other person who provides services to the Bank, is barred from disclosing to the client or any third party that a criminal investigation is in progress or that it has transmitted any information to the authorities or, further, any internal or external information material for the prevention, investigation and detection of money laundering.

This duty does not prevent the disclosure of information to entities belonging to the same business Bank, the competent authorities, or other relevant financial entities, provided this is made for anti-money laundering purposes.

7.10. Duty to provide training

The Bank, through the Compliance Department, should adopt the actions necessary so that its bodies, the relevant employees, and the employees whose functions are directly related to anti-money laundering purposes have appropriate knowledge of the obligations resulting from the legislation and regulations in force.

The anti-money laundering and terrorist financing training plan should be designed on a pluri-annual basis and provide regularly for: (i) training of new employees; and (ii) training of relevant employees.

8. AML/CFT Global Risk Management Model

The principal responsibility for the Bank's ML/FT risk management lies with the Board of Directors, responsible for defining and overseeing the Bank's AML/CFT internal rules and allocating operational responsibilities and resources under the "three lines of defense" model.

The Bank's AML/CFT controls and procedures follow a risk-based approach, which requires the identification and assessment of the risks at hand and the application of specific mitigation measures.

Compliance with" Know Your Client" due diligence measures, including the collection and verification of client information and the monitoring of client transactions.

Documenting and record-keeping of all information obtained through client and transaction due diligence, thus, ensuring proper audit trail and fostering sound supervisory reporting.

Preventing, detecting, and combating ML/FT, as well as Sanctions and Restrictive Measures requires the definition of a specific governance model that allows the identification, monitoring and control of ML/FT risks and Bank Restrictive Measures ensuring functional segregation between the competencies and responsibilities of the bodies involved.

Therefore, and to comply with the principle mentioned above, the Bank operationalizes the governance of ML/FT risk and Restrictive Measures with the establishment of 3 lines of defense and ensuring through this Regulation the definition of their respective powers and responsibilities.

8.1. Risk Management

The Bank has an AML assessment methodology, the Compliance Department being responsible for:

a. identifying the actual risks of money laundering, including risks related to:
   i) the nature, size and complexity of the Bank's business;
   ii) its respective Clients;
   iii) the business areas pursued, as well as the products, services and transactions offered;
   iv) the distribution channels of the products and services offered, as well as the means of communication used to contact clients;
   v) the countries or territories of origin of the Bank's clients or where such clients have their domicile or otherwise carry out their business;
   vi) the countries or territories where the Bank operates either directly or through third parties, belonging to the same Bank or otherwise;

b. assessing the risk of money laundering, including by determining:
   i) the degree of probability and the impact of each risk specifically identified, taking into account to this end all material variables in the context of its operating circumstances, including the purpose of the business relationship, the level of assets deposited by client or the volume of transactions carried out and the regularity or duration of the business relationship;
   ii) the overall risk of the Bank and of its respective business areas;

c. establishing and adopting any means of control and control procedures that prove to be appropriate to mitigate the specific risks identified and assessed, adopting particularly enhanced procedures in the event of any increased risk of money laundering;

d. reviewing risk management practices and ensuring they are up to date.

Risk management practices, as well as their respective updating must be proportionate and documented by means of written documents that reflect the risks underlying the Bank's business.

In this context, particular attention must be paid to any risks of money laundering that might result from offering products or transactions which favor anonymity, the development of new products and business practices and the use of new technologies.

8.2. Effectiveness Assessment

The Bank ensures periodic and independent assessments of the quality, adequacy, and effectiveness of the AML/CFT policies, procedures and controls, including:

- the AML/CFT risk assessment model;
- the identification, due diligence and retention procedures adopted;
- the integrity, timeliness and comprehensibility of the reports and communications generated by the information systems;
- the adequacy of the client and transaction monitoring procedures and controls;
- the adequacy, comprehensiveness, and timeliness of the procedures to examine and report suspicious transactions;
- the internal training policy;
- the quality, adequacy, and effectiveness of the performance of processes, services or activities outsourced to third-party service providers;
- the speed and sufficiency of the procedures to correct shortfalls previously detected in audit or supervision actions; and
- the quality of the reports and other information submitted to the Bank of Portugal.

These assessments shall be conducted on an annual basis, have an extension proportionate to the nature, size and complexity of the Bank and be performed by the internal audit function, external auditors or duly qualified third parties.

8.3. Clients ML/FT risk scoring

The Bank has defined parameters that it has implemented in its IT systems, which ensure the definition and updating of the risk profile associated with Clients.

A classification based on the pre-defined rules is hereby laid down for the purposes of onboarding new Clients, and/or whenever an update of the client information is performed in the system.
The following categories are set for individuals and entities[5]:

- High Risk
- Medium Risk
- Low Risk.

8.4 Information systems

The Bank has appropriate and up-to-date information systems, which enable the Bank:

- to record all identification data and other information concerning its Clients, Counterparties, representatives, and beneficial owners;
- to identify, by filtering its Database against the most relevant PEP list provided by Dow Jones FACTIVA, as well as the United Nations (UN), the OFAC, the European Union (EU) and Bank of England Sanctions lists;
- to assign a money laundering risk score to each client;
- to monitor and detect transactions which may constitute a money laundering or terrorist financing offence.

8.5. Whistleblowing system

The Bank has implemented a whistleblowing system that enables its Employees to report any fault related to a possible breach of legal or regulatory provisions or internal policies or procedures.

This system corresponds to a specific, independent, and anonymous channel that ensures the reception, handling and filing of reports.

[5] Includes their respective proxyholders, mandataries, agents or other forms of representation.

8.6. Monitoring of branches and affiliates

The Bank has procedures for the monitoring of its branches and affiliates abroad by the Compliance Department, as laid down in the internal Regulation Compliance Report by Geography.

In accordance with the aforementioned rules, the Compliance Department receives monthly reports from the local heads of the Compliance function containing all information required, in particular in respect of AML/CFT. Thereafter, monthly meetings or videoconferences are held with representatives of the Bank's units to discuss the issues stated in the reports, the information being compiled and submitted to the Executive Committee each month.

8.7. Independent Testing

Adherence to the requirements of the AML regulation is subject to independent testing by Haitong Internal Audit function and the Annual External Year-End Auditor.

9. Client Onboarding

a. Classification Rules

i. Prohibited Business Relationship

Individuals or entities who/which fall under or present signs of falling under any of the following types cannot be accepted as Clients and the existence of any relationship, be it merely prospective or exploratory, with any individual or entity of this nature must be reported immediately to the Compliance Department.

It is prohibited to:

1- accept Assets that are known or suspected to be the proceeds of Criminal Activity;
2- enter into or maintain Clients Relationships with Natural Persons or Non-Natural Persons known or reasonably suspected to be:
   - involved in terrorist activity or its funding;
   - involved with a criminal organization or members of such or persons associated with such in any capacity;
   - engaging in or facilitating Criminal Activity (including Tax Evasion offences for themselves or as an agent for – or otherwise on behalf of – others);
   - listed on relevant Sanctions lists;

- involved in or linked to controlled drugs (e.g. medical marijuana) where the drugs are illegal in the jurisdiction; or
- Gambling entities that are not licensed or government regulated.

3. Enter into or maintain relationships where:
   - The true identity of the Client (including UBO), cannot be obtained;
   - The purpose and nature of the relationship cannot be established or does not appear to be legitimate;
   - There are doubts about the veracity of documents or information obtained for the purpose of identification or Verification;
   - The Client has connections with certain prohibited special risk countries (related to sanctions and restricted measures);
   - The Client conducts activities or operations in prohibited industries;
   - The business does not believe they can effectively manage the Financial Crime Risks of the Client;
   - individuals or entities, including beneficial owners, mentioned in official lists related to anti-money laundering and terrorist financing and/or mentioned in the list drawn up by LSEG *World-Check Database*[6] as being associated with illegal activities. For this purpose, the following official lists published to this end by the European Union, the United Nations Security Council, the US authorities (OFAC, Office of Foreign Assets Control), the UK Sanctions List and the Bank of Portugal must cumulatively be taken into account.
   - Individuals or entities, including beneficial owners, who/which have any activity whose nature makes it impossible to confirm the legal origin of their respective income.
   - Individuals or entities who/which are not physically present at the time of establishing the business relationships, except when they are duly represented and without prejudice to relationships established at a distance in accordance with Schedule I to Notice no. 1/2022.
   - Individuals or entities who/which refuse to provide information or documentation requested by the Bank or required by law.
   - Individuals or entities who/which perform illegal activities.
   - Individuals who lack mental capacity, not duly represented by a person with powers and authority to such end.

[6] Specialist database subscribed by the Bank to this end.

- Individuals or entities who/which clearly lack economic capacity to perform the proposed transactions.
- Entities which have definitively ceased their business (applies only to new Clients).
- Unauthorised financial or similar entities.
- Entities dissolved or in the course of liquidation (applies only to new Clients).
- Entities which run unauthorised gambling activities.
- Entities terminated (applies only to new Clients).
- Entities whose share capital is represented in whole or in part by bearer shares.
- Shell Bank[7].

ii. High Risk

The following prospective Clients are deemed High-Risk Clients and must, therefore, be subject to enhanced due diligence procedures:

- Clients classified as such under the Client scoring mechanism in force within the Bank's tools, for the purposes of assessment of the money laundering and terrorist financing risk.
- Residents in countries subject to any embargo decreed by the European Union and the USA (applicable not only to prospective Clients, but also to their respective representatives or co-owners) stated in the following official lists issued by the European Union, the United Nations Security Council, the OFAC or as notified by the Bank of Portugal.
- Residents in territories classified as tax havens, as listed in Finance Ministerial Order no. 150/2004 or any provisions substituted therefor.
- Residents in territories classified as offshore for the purposes of Finance Ministerial Order No. 150/2004 or any provisions substituted therefor.
- Residents in countries classified as non-cooperative, in accordance with the lists published by the Financial Action Task Force (FATF).
- Individuals or entities associated with: *i)* the production or distribution of weaponry and other military equipment; *ii)* the production or proliferation of weapons of mass destruction.
- Politically exposed persons (hereinafter "PEPs") and other senior political or public officers[8].

[8] PEPs within the meaning of article 2(2)(cc) of Law no. 83/2017 and other senior political or public officers within the meaning of article 2(2)(gg) of Law no. 83/2017.

- Individuals or entities who/which perform activities involving a high risk of being used for the purposes of money laundering or terrorist financing, their officers, shareholders or owners, such as, for instance: casinos or duly authorised bookmakers, foreign exchange firms, pawnbrokers and money transfer firms.

The aforementioned circumstances should be analysed by the Bank's bodies responsible for approving new Clients and/or transactions before commencing any business relationship with any entity presenting signs of possibly falling under one of the aforementioned types.

iii. Medium Risk

The following prospective Clients are deemed Medium-Risk Clients:

- Clients classified as such under the Bank's Client scoring mechanism.
- Any entities belonging to the Haitong Bank S.A.'s or its holding companies.
- Employees and officers of entities belonging to the Haitong Bank, S.A.

iv. Low Risk

The following types of Clients are deemed Low-Risk Clients, provided they are located in Portugal, in European Union Member States or third countries with effective AML/CFT systems.

- Management bodies or state-owned companies.
- Financial entities [9] (including their branches, provided they comply with the procedures determined by the holding company), except payment institutions and insurance brokers.
- Companies whose shares are admitted to trading on a regulated market (including branches and affiliates subject to their exclusive control, provided such control is documented) and subject, by virtue of the rules of such market, the law and other mandatory instruments, to duties to inform that ensure appropriate transparency in respect of beneficial owners [10].
- Individuals with term deposit accounts limited to € 100.000, obtained through the online platforms of Raisin.

[9] Within the meaning of Article 3(1) of Law No. 83/2017.
[10] In order to identify the regulated markets that ensure appropriate transparency, the Bank must use the information made available by the supervisory authorities of the sector in question.

Simplified due diligence procedures[11] may be applied to these entities in terms of identification and due diligence procedures (hereinafter "Know Your Client" or "KYC") and monitoring of transactions.

b. Client Classification Procedure

The Client classification in line with the rules applying to the aforementioned categories should be calculated upon recording the counterparty in the central database, on the basis of the data:

i. contained in the documentation and instructions received from the employees of the relevant Front Office area.

ii. Whenever the Front Office area collects indicia that a Client may be "High Risk", his/her/its file must be forwarded to the Compliance Department, which will analyse the case and take any additional actions deemed appropriate in line with the increased risk presented by the Client, duly documenting its analysis in writing in accordance with the applicable internal template.

iii. It is expressly forbidden to establish any business relationship (even if merely of an exploratory or prospective nature) with prospective Clients who/which the Bank is able to identify as being "Unacceptable".

iv. Any contact, even if merely of an exploratory or prospective nature, with prospective Clients classified as "Unacceptable" must be reported immediately to the Compliance Department.

10. Know Your Client

In accordance with the regulations in force, each financial entity is bound to thoroughly identify its Clients, know their business activities, know their respective ownership and control structures, as well as to verify whether the relationship with these entities is consistent with the nature and volume of the business carried out.

To this end, the KYC procedures implemented in the Bank must be strictly and fully adhered to before any services are provided to the Client.

Employees of the Front Office areas are responsible for adhering to the KYC procedures determined for each category of Client and must ensure that the data collected from Clients is sufficient, as well as that it truly reflects Clients' circumstances, notably in respect of their identity, business and financial capacity.

[11] Within the meaning of article 35 of Law no. 83/2017.

The employees of the Front Office area responsible for the Client are responsible for ensuring that all the respective information and documentation are kept duly updated, meeting the applicable deadlines in line with the money laundering and terrorist financing risk profile assigned to the Client:

- low AML/CFT-risk Clients – every 5 years;
- medium AML/CFT-risk Clients – every 3 years;
- high AML/CFT risk-Clients – every year.

Notwithstanding the periodic review cycles set out above, the Client's information, documentation and ML/FT risk classification must be reviewed whenever the Bank becomes aware of a material change or relevant event, including changes in ownership or control, beneficial ownership, activity, transaction profile, source of funds or wealth, geographical exposure, PEP status, sanctions exposure or adverse media.

The assessment referred to in the preceding paragraphs must be periodically updated by the employee responsible for the business relationship, in line with data gathered from time to time from the monitoring of the Client, and he/she must periodically ask the Client for any additional data which proves necessary and/or useful for such assessment.

a. Low Risk

- Operations Department validates the mandatory information and documentation of the KYC process.
- Operations Department conducts searches against the LSEG WorldCheck international lists to check for sanctions, restricted measures, PEP status or adverse media.
- Operations Department conducts a four eyes principle review of the KYC process within the client database system ("SAP-MER") in order to confirm that the information recorded in the system is compliant with the documentation submitted by the Client.
- Compliance Department may also have intervention on this process when the Clients are subject to the Adoption or Credit Committees, in which case the Compliance Department searches for adverse media in publicly available information, consults reliable and independent sources (e.g., Informa D&B) and double checks if the Client has any connection with jurisdictions subject to restrictive measures.
- Update of KYC information must be performed every 5 years.
- In case the Client AML risk increases for High, the process is escalated to the Compliance Department to conduct an enhanced due diligence.

- In the course of the business relationship, the Bank's client database is screened, on a daily basis, against the international Sanctions and Restricted Measures lists and against the national and international PEP list. In case of a positive match for PEP, the client is classified accordingly within SAP-MER and enhanced due diligence is performed.
- In the course of the business relationship, wire transfers are filtered against international lists of Sanctions and Restrictive Measures; If any positive match occurs, the transfer could be refused, or additional information / documentation may be requested to the Client, in order to perform enhanced due diligence on the KYC process.
- According to the rules previously defined by the Bank, KYT alerts are issued by the FISERV monitoring system and whenever necessary additional information/documentation could be requested to the client through the Relationship Manager in order to justify the specific transaction and understand if the flow performed in the account matches to what was expected at the beginning of the business relationship.

During the analysis performed by Compliance, if necessary, in addition to the above-mentioned measures, the following enhanced due diligence measures may be applied:

- the risk scoring of the Client could be increased manually in the SAP-MER, core system and the Bank, and an enhanced due diligence should be performed by Compliance Department; This action will reduce the time for the next KYC review date.
- the account could be set to "Close Monitoring" in the FISERV, transaction monitoring system of the Bank, and therefore, all the transactions that take place in the clients account will issue an alert that will have to be analysed by Compliance.

b. Medium Risk

All of the above measures apply to medium-risk clients, with the only difference being that, for medium-risk clients, the regular update period of the KYC process is reduced to 3 years.

c. High Risk

Generally, the most common situations that are at the basis of a high-risk client classification are related with (i) the country of incorporation of an entity or the residence of an individual, (ii) the complex structure of the entity and (iii) the fact that the client is a PEP.
In those situations, the following actions are to be followed:

a.1. The relationship manager (“RM”) should collect information and/or documentation regarding the source of funds relating to the initial deposits and subsequent funding of the account, namely:
- the amount expected.
- the activities that generated the funds for the Client relationship e.g., proof of regular remuneration (e.g., salary or a balance sheet) and/or proof of the origin of funds that will be used for subscribing the products of the Bank (e.g., documentation that prooves the selling of shares of a Company, an inheritance, etc.).
- the country from which the fund transfer(s) originate(s).
- remitting party and, where applicable, the financial institution from where the transfer originated.
- in case of PEP, the process has to include an e-mail from a Business Senior Manager where he/she consider whether or not to provide their approval to establish or continue the Client Relationship.
The Compliance Department should analyze the information/documentation collected and perform additional searches, in addition to the ones conducted at the 1st phase of the onboarding, search for adverse media in publicly available information, consult reliable and independent sources (e.g., Informa D&B) and double check if the Client has any connection with jurisdictions subject to restrictive measures.
When the client is a legal entity or a legal arrangement, the Bank must obtain satisfactory knowledge of the client's beneficial owners and keep written records of all actions taken to this end.

Legal entities that establish or maintain business relationships or perform occasional transactions with the Bank must supply in due course: (i) information on their legal or formal owner; (ii) sufficient, accurate and current information on their beneficial owners; (iii) particulars on the nature of the control exercised by the beneficial owner and the underlying economic interests; and (iv) any other documents, data and information required for the Bank to comply with the applicable regulations.

The Bank must ensure any procedures necessary to consult the Central Register of Beneficial Owners.

10.1. Simplified measures

The Bank may, after having identified a demonstrably low risk of ML/FT, take simplified measures under the duty to identify and apply due diligence measures. Simplified measures means, for instance:

a. verification of the client's and the beneficial owner's identification after establishment of the business relationship;
b. reduction in the frequency for updating details collected in compliance with the duty to identify and apply due diligence measures;

c. reduction in intensity of the ongoing monitoring and in the depth in which transactions are analyzed in the event of the sums involved being low;
d. non-collection of specific information and non-application of specific measures making it possible to understand the purpose and the nature of the business relationship, where such purpose and nature can be reasonably inferred from the type of transaction made or from the business relationship established.

The measures adopted must be consistent with the low risk factors identified.

10.2. Enhanced due diligence measures

While having determined initially the Client / Counterparty risk profile, the Bank must be watchful of the indicators suggesting increased risk of ML/FT.
Enhanced measures must be adopted when the Client is classified as a High risk Client in the system, and as risk based approach, when a higher risk of money laundering is identified in the business relationships, the occasional transactions or the transactions carried out.
When the client has a high-risk classification, it has always to be escalated to local Compliance Department;
Enhanced measures mean, for instance:

a. Conduct additional screening searches;
b. Conduct searches for adverse media;
c. obtaining additional information on clients or their representatives or beneficial owners, as well as on transactions planned or carried out and the nature of the business;
d. taking additional steps to verify the information obtained;
e. verify the source of funds;
f. check the source of wealth;
g. examine the purpose of the transaction;
h. re-evaluate the Client Risk Assessment,
i. involvement of higher hierarchical levels to authorize the establishment of business relationships, the carrying out of occasional transactions or transactions in general;
j. increase in the depth or frequency of the monitoring procedures applied to the business relationship or certain transactions or set of transactions, with a view to detecting possible indicators of suspicion and subsequently complying with the duty to report;
k. reduction in the time intervals for updating information and other details collected in the course of compliance with the duty to identify and apply due diligence measures;

l. authorize the monitoring of the business relationship by the money laundering reporting officer or another employee that is not directly involved in the business relationship with the client;
m. requirement that the first payment concerning a certain transaction be made by traceable means with origin in a payment account opened by the client with a financial entity or any other duly authorized entity that, not being situated in a higher-risk third country, has demonstrably applied equivalent identification and due diligence measures.

10.3. Politically exposed persons

In the context of their business relationships or occasional transactions with clients or their representatives or beneficial owners who are politically exposed persons (PEPs), by way of supplement to the standard identification and due diligence procedures, the Bank shall:

a. detect the PEP status acquired before or after establishment of the business relationship or the carrying out of the occasional transaction;
b. ensure approval by a member of its senior management for (i) establishing business relationships or carrying out occasional transactions; (ii) continuing business relationships with such persons when they become politically exposed persons after establishment of the business relationship;
c. take adequate measures to establish and verify the source of wealth and of funds that are involved in the business relationships, occasional transactions or transactions in general;
d. conduct enhanced, ongoing monitoring of business relationships, in particular with a view to identifying any transactions that should be reported.

The Bank shall also register in its systems the holders of other political or public offices that do not qualify as politically exposed persons, as listed in articles 2 and 3 of Law No. 52/2019, and apply the due diligence measures previously identified, in particular when a higher risk of ML/FT is identified.

Close business associates include:

a. natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements with a PEP;
b. natural persons who own share capital or voting rights in a legal entity or assets of legal arrangements which are known to have been set up for the de facto benefit of a PEP;
c. natural persons who are known to have corporate, business or professional relations with a PEP.

In a conservative approach, the Bank may identify and classify as PEPs in a database any other categories of persons who present characteristics that might suggest political exposure.

10.4. Additional due diligence

In addition to the identification of clients, counterparties, representatives and beneficial owners, the Bank's employees must:

a. take appropriate action to understand the client's ownership and control structure, where the client is a legal entity or a legal arrangement;
b. obtain information on the purpose and purported nature of the business relationship;
c. obtain information, when the risk profile of the client or the characteristics of the transaction so advise ("high risk" or, potentially, "unacceptable"), on the origin and destination of any funds transferred within a business relationship or execution of an occasional transaction;
d. continuously monitor the business relationship, so as to ensure that these transactions are consistent with the institution's knowledge of the client's activities and risk profile; and
e. update any information details obtained in the course of the business relationship.

10.5. Performance by third parties of the duty to identify and due diligence

If the Bank decides to hire a third party to perform the identification and due diligence procedures, the Bank must ensure:

a. that the third party is an entity covered by Law no. 83/2017, is authorized to perform identification and due diligence procedures and is reliable, there being no publicly known information which might affect its reputation;
b. that it collects complete information on the clients from the third party or performs a new identification, in the event of insufficiency of the information or if the associated risk so advises;
c. compliance with all record-keeping requirements laid down article 51 of Law No. 83/2017, as if the identification and due diligence procedures performed by the third-party were performed by the Bank itself;
d. that the third party:
    i) gathers all the information and performs all identification, due diligence, and record-keeping procedures that the Bank must observe itself;
    ii) immediately provides a copy of the identification and identity verification data and other relevant documentation on the client and his/her/its representatives and beneficial owners that were the subject of identification and due diligence procedures;
    iii) has an appropriate AML/CFT internal control system;

iv) has the necessary human, material and technical resources to perform the identification and due diligence procedures face-to-face or at a distance, as the case may be;
v) has employees with appropriate AML/CFT training;
vi) identifies the employee who performed the duty to identify and to apply due diligence measures and the date of such performance;
vii) collects the identification details of clients and their representatives or beneficial owners before the business relationship is established.

This assessment shall be prepared by the Compliance Department and a final report shall be completed.

11. ARCHIVE

This Regulation, and all the associated documents, are subject to the general archiving rules laid down in the procedure PM220 – Archive Management.

12. DISCLOSURE

This Regulation is available on intranet and any change to the same should be duly communicated by e-mail to all the Bank's employees.

13. CONTROL OF VERSIONS

Table 1: Information about the Document	
Name of the Document	Anti-Money Laundering and Countering the Financing of Terrorism Regulation
Version	Version 6.0
Prepared by (Name/Department)	Compliance Department
Appreciated on (Committee name)	CA on 11/11/2026 and CGC on 10/11/2026
Approved by (Committee name)	Board of Directors

Table 2: Versions' update

Version no.	Date	Written by:	Approved by:	Nature of Change
1.0	11/08/2014	Compliance Department	Board of Directors	**Initial version**

2.0	20/03/2017	Compliance Department	Board of Directors	Review of initial version Review of links and applicability Additions: Schedules III to V
2.1	28/11/2017	Compliance Department	Executive Committee	Review of 2.0 Review of links and the applicable legislation, notably Law No. 83/2017 of 18 August
2.2	05/02/2019	Compliance Department	Executive Committee	Review of 2.1 Annual review of links and of the legal and regulatory framework, notably Notice no. 2/2018 of the Bank of Portugal.
2.2	15/09/2020	Compliance Department	Board of Directors	Ratified by the Board of Directors
3.0	02/03/2022	Compliance Department	Board of Directors	New Template; Update legal and regulatory references; Section 7.2.1 was added: Compliance Department participation in relevant business forums; Elimination of the extensive list of PEP functions, replaced by a reference to the legal requirement; Update of schedules 1 and 2 in accordance with Bank of Portugal's Instruction 2/2021.
3.1	14/10/2022	Compliance Department	Board of Directors	Annual review; update legal and regulatory references due to new Bank of Portugal Notice 1/2022; Update of schedules 1 and 2 in accordance with Bank of Portugal's Notice 1/2022.

4.0	25/06/2024	Compliance	Board of Directors	Annual review; general amendments and merge of Client Acceptance Regulation within this document. Revokes Regulation No. COM.R04 – Client Acceptance Regulation
5.0	10/09/2025	Compliance	Board of Directors	Annual review
6.0	11/11/2026	Compliance Department	Board of Directors	Annual revision; Integration of Regulation No. COM08.R09 Anti-Money Laundering and Countering the Financing of Terrorist ("AML/CFT") Risk Assessment Methodology into this Regulation as an Annex. Revokes Regulation no. COM08.R09.

Schedule I - Illustrative list of factors and types indicating a potentially lower risk

(attached to Law no. 83/2017 and Bank of Portugal's Notice 1/2022)

1 — Client risk factors:

a) companies whose shares are admitted to trading on a regulated market and subject, by virtue of the rules of such market, the law and other mandatory instruments, to duties to inform that ensure appropriate transparency in respect of beneficial owners;
b) public administration or state-owned companies;
c) clients residing in lower-risk geographies, identified in line with no. 3 of this schedule;
d) Clients with a simple control and ownership structure that allows easy and timely knowledge of information regarding their beneficial owners;
e) Clients subject to information disclosure requirements in line with European Union law or subject to equivalent international standards, which ensure sufficient transparency of information regarding the respective beneficial owners;
f) Clients with assets and investments of reduced amounts.

2 — Product, service, transaction or distribution channel risk factors:

a) life insurance, pension fund or similar savings product agreements with a low premium or annual contribution;
b) insurance agreements associated with pension funds, provided they neither have a redemption clause nor can be used as security for loans;
c) pension, complementary pension or similar schemes to pay retirement pensions to employees, whose contributions are deducted from salaries and with rules prohibiting the assignment of rights;
d) limited and clearly defined financial products or services with a view to increasing the level of financial inclusion of certain types of clients;
e) products in which the money laundering and terrorist financing risks are controlled by other factors, such as limits in terms of sums that may be credited or the transparency of their ownership, including certain types of electronic currency;
f) non-complex financial products with low profitability or return;
g) products of limited use or specific and predetermined purposes, such as:
    - fixed-term savings products with low savings thresholds;
    - products whose benefits can only be realized in the long term or for a specific reason, such as retirement or the acquisition of a property for own and permanent housing;

- products made available to certain categories of Clients who meet pre-defined circumstances, for example, beneficiaries of social benefits, parents representing their children, or minors until they reach the age of majority.
- recurring transfers of an identical amount and to the same beneficiary, with apparent economic rationality, including payment of essential minimum services, payment of salaries and contributions to pension funds;
- products that do not allow cash refunds;
- products that can only be used in national territory;
- products that can only be used to acquire goods or services, namely when the acquisition of goods or services by their holder can only take place in a limited number of merchants or points of sale and the financial entity has sufficient knowledge of the activities carried out by the merchants;
- low value credit products, including those conditioned to the purchase of a good or service;

h) Pooled accounts held by Clients who meet the requirements set out in paragraph c) of no. 1 of Annex II of the Law, determined in accordance with the provisions of paragraph c) of no. 1 of Annex II, and demonstrate that they are in a position to immediately provide information and documents relating to their own Clients, in compliance with identification and diligence measures compatible with those provided for in the Law and in this Notice;

i) Payment initiation services;

j) Account information services.

3 — Geography risk factors

a) European Union Member States;

b) third countries with effective money laundering and terrorist financing systems;

c) countries or jurisdictions identified by reliable sources as having a low level of corruption or other criminal activities;

d) third countries subject, on the basis of reliable sources, such as published mutual assessment, detailed assessment or monitoring reports, to obligations to prevent money laundering and terrorist financing consistent with the FATF's revised recommendations and which effectively implement such obligations.

Schedule II - Illustrative list of factors and types indicating a potentially higher risk

(attached to Law no. 83/2017 and Bank of Portugal's Notice 1/2022)

1 — Client risk factors:

a) business relationships taking place in unusual circumstances;
b) clients residing or doing business in higher-risk geographies, identified in line with no. 3 of this schedule;
c) legal entities or legal arrangements used as a means to hold personal assets;
d) companies with nominee shareholders or whose capital is represented by bearer shares;
e) clients who/which carry out activities involving involved cash-intensive transactions;
f) corporate ownership or control structures that appear unusual or excessively complex taking into account the business carried out by the client;
g) Clients who are non-profit organizations and who have been identified, pursuant to Article 145(3)(a) of Law No. 83/2017, as representing an increased risk of money laundering or financing of terrorism;
h) Clients residing or operating in jurisdictions associated with a higher risk of money laundering or terrorist financing;
i) Clients with nationality in jurisdictions associated with a higher risk of financing terrorism or supporting terrorist activities or acts;
j) Clients with known links to foreign terrorist fighters;
k) Clients who carry out economic activities with dual-use goods;
l) Clients who carry out economic activities in sectors prone to tax evasion or who are considered, by reputable and credible sources, as having a high risk of money laundering and terrorist financing (e.g. real estate, gambling, transport, auctions, among others);
m) Clients who carry out economic activities in sectors often associated with high levels of corruption;
n) Clients who use intermediaries or agents with broad powers of representation, for the purposes of initiating or managing the business relationship, especially when they are based in jurisdictions associated with a higher risk of money laundering or terrorist financing;
o) Clients who are newly created legal entities and without a known business profile or suitable for the declared activity;
p) Clients that are asset holding vehicles or asset management vehicles;
q) Clients who have been subject to measures or sanctions of an administrative or judicial nature for violating the regulatory framework related to money laundering or terrorist financing.

2 — Product, service, transaction or distribution channel risk factors:

a) private banking;
b) products or transactions which might favour anonymity;
c) payments received from third parties unknown or not related to the client or the business carried out by the client;
d) new products and new trade 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;
e) products or services associated with virtual assets;
f) products, services, operations or distribution channels that are characterized by an excessive degree of complexity or segmentation;
g) high-value cash transactions, mainly using high denomination banknotes;
h) one-off operations of high value, taking into account what is expected for the product, service, operation or distribution channel used;
i) products without delimited geographical use, even if this is not necessary for the execution of the respective purposes;
j) credits guaranteed by assets that are in jurisdictions that make it difficult or prevent obtaining information regarding the identity and legitimacy of the parties involved (and respective beneficial owners) in providing the guarantee;
k) circuit of funds with a high number of intermediaries operating in different jurisdictions;
l) electronic money products without limitation with regard to:
    - number or amount of payments, shipments or refunds allowed;
    - electronically stored monetary value;
m) operations financed using anonymous electronic money, including using electronic money products that benefit from the exemption provided for in article 12 of Directive (EU) 2015/849, of the European Parliament and of the Council, of 20 May 2015;
n) electronic money products or other prepaid instruments that allow the transfer of funds between different users;
o) the creation or use of asset holding vehicles or asset management vehicles.

3 — Correspondent banking risk factors

a) correspondent relationships in which the respondent – or the financial Bank he is part of – has been subject to measures or sanctions relevant to the prevention of money laundering and terrorist financing;
b) situations in which the respondent develops a significant segment of its business in activities or

sectors frequently associated with money laundering or terrorist financing;

c) correspondent relationships with entities that hold an offshore banking license.

4 — Geography risk factors

a) jurisdictions identified by reputable and credible sources as having ineffective judicial systems or deficiencies in the investigation of crimes associated with money laundering or terrorist financing;
b) jurisdictions that do not implement reliable and accessible registers (or other equivalent mechanisms) of beneficial ownership;
c) jurisdictions that have not implemented the Common Reporting Standard developed by the Organization for Economic Co-operation and Development (OECD), relating to the automatic exchange of information (Common Reporting Standard);
d) jurisdictions known for offering simplified or non-existent relevant administrative procedures or clearly more favorable privileged tax regimes;
e) jurisdictions with legal regimes that establish prohibitions or restrictions that prevent or limit compliance, by the financial entity, with the legal and regulatory rules that govern its activity, including the provision and circulation of information.

Schedule III - Illustrative list of potential suspicion indicators

(available in the portal of the Money Laundering and Terrorist Financing Policy Coordination Committee[12])

A. GENERAL INDICATORS

- Clients who/which have business relationships, execute occasional transactions or execute transactions in general that – due to their nature, frequency, amounts involved or any other factor – are inconsistent with their profile.
- Clients who/which, without any reasonable explanation, handle cash: (a) in unusual amounts; (b) in amounts inconsistent with their profile; (c) wrapped or packaged in an unusual way; (d) in poor condition; or (e) represented by small denomination banknotes, with a view to exchanging them for higher denomination banknotes.
- Clients who/which, in any way whatsoever, seek to persuade the financial institution's employees to ignore any AML/CFT legal obligation or internal procedure.
- Clients who/which are reluctant or refuse to provide identification details/evidence/other information particulars or to take any verification action deemed necessary by the financial institution to:
    - identify the client, his/her/its representative or the beneficial owner;
    - understand the client's ownership and control structure;
    - know the nature and purpose of the business relationship;
    - know the origin and destination of the funds; or
    - characterise the client's business.
- Clients who/which are reluctant or refuse to provide original or equivalent documents.
- Clients who/which are reluctant or refuse to update their information details.
- Clients who/which are reluctant or refuse to deal face-to-face with the financial institution.
- Clients who/which provide identification details, evidence or other information details which:
    - are unreliable as to their authenticity;
    - are unclear as to their content;
    - are difficult to verify by the financial institution; or

[12] http://www.portalbcft.pt/sites/default/files/anexos/indicadores_suspeicao_genericos_1.pdf

  - present unusual characteristics.

- Clients who/which present different identification documents each time the same are requested by the financial institution.
- Clients who/which, in the course of their business, use pseudonyms, nicknames or any alternative expressions other than their true name or designation.
- Clients who/which postpone or do not deliver any documentation that may be submitted to the financial institution after the business relationship is established.
- Clients who/which seek to suspend or alter the business relationship or the occasional transaction after the identification details and their respective evidence or other information details relevant to know the client are requested of them.
- Clients who/which do not wish any correspondence to be sent to their stated address.
- Clients who/which, being apparently unrelated, give identical addresses or contact details (telephone number, fax number, email address or other details).
- Clients whose address or contact details (telephone number, fax number, email address or other details) prove to be false or are permanently inactive, particularly when the financial institution tries to contact them shortly after the business relationship is established.
- Clients whose address or contact details (telephone number, fax number, email address or other details) change frequently.
- Clients who/which appear to be acting on behalf of a third party without, however, disclosing it to the financial institution or, if they do, refuse to supply the necessary information details on the third party on whose behalf they are acting.
- Clients who/which seek to establish close relationships with employees of the financial institution.
- Clients who/which seek to restrict their contacts with the financial institution to one or more specific employees of the financial institution, in particular when – if this or these employees are absent – they decide not to execute or suspend any transaction.
- Clients who/which show unusual knowledge of money laundering and terrorist financing legislation.
- Clients who/which evidence uncommon interest in knowing the financial institution's AML/CFT policies, procedures and internal controls.
- Clients who/which, within a short period of time, have started similar business relationships with different financial institutions.

- Clients who/which carry out their business in different successive locations, apparently trying to avoid their detection by third parties.
- Clients who/which recurrently execute transactions to an amount below the limits that would trigger adoption of identification procedures[13].
- Clients who/which purchase valuable goods and sell the same within a short period without apparent reason.
- Clients who/which, on the same day or within a short period of time, execute transactions in different branches of the institution.
- Clients who/which give unclear or inconsistent explanations about transactions or are not familiar with their purpose.
- Clients who/which give excessive and unsolicited explanations about transactions.
- Clients who/which evidence nervousness or unusual urgency in executing transactions.
- Clients related to transactions suspected of ML/FT, notified by the financial institution to the competent authorities.
- Clients related to transactions suspected of ML/FT, notified by the supervisory authorities under article 40 of the Law and of which the financial institution is aware.
- Clients who/which are being or have been investigated for criminal activities, in particular ML/FT or any offence underlying the latter (provided this information is directly known by the financial institution or obtained from a reliable public source).
- Clients explicitly mentioned by the competent authorities as potentially related to ML/FT activities.
- Clients who/which carry out any sort of financial activity without being duly authorised or skilled to this end.
- Transactions evidencing a degree of complexity apparently unnecessary for the purpose for which they are intended, due to, *inter alia*, the number of financial operations, financial institutions, accounts, parties and/or countries or jurisdictions involved.
- Transactions for no apparent purpose or economic reason.

[13] The Bank adopts identification procedures for all clients and counterparties with whom/which it deals, irrespective of the amount of the transaction in question.

- Transactions whose frequency, unusualness or exceptionalness have no plausible reason in light of the client's profile.
- Transactions apparently inconsistent with current practice in the client's industry or business.
- Transactions involving shell companies.
- Transactions unrelated to the client's known business and involving persons or entities related to countries or jurisdictions publicly known as:
    - places of production of / trafficking in narcotics;
    - having high levels of corruption;
    - money laundering hubs;
    - sponsoring or supporting terrorism; or
    - sponsoring or supporting the proliferation of weapons of mass destruction.
- Transactions unrelated to the client's known business and involving persons or entities related to the countries, territories or regions with highly favourable tax systems contained in the list in Ordinance No. 150/2004 of 13 February or other countries or jurisdictions with highly restrictive banking secrecy legislation.
- Business relationships or occasional transactions in which it is sought to disguise the identity of the beneficial owners, notably through complex shareholding structures.

B. INDICATORS RELATED TO BANK DEPOSIT ACCOUNTS

- Clients who/which maintain a considerable number of bank deposit accounts open, in particular when some remain dormant for long periods.
- Clients who/which have bank deposit accounts with several credit institutions located in the same country/geographic area.
- Clients who/which make deposits without accurately knowing the sums to be deposited.
- Clients who/which open accounts with significant amounts of cash.
- Clients who/which frequently use personal accounts to execute transactions related to their business activity.
- Accounts frequently presenting operations for which the relevant accountholder gives no reasonable explanation.
- Accounts opened in branches geographically distant from the client's address or work place.

- Accounts whose operations largely exceed those foreseeable at the time they were opened.
- Accounts co-owned or operated by a high number of persons personally or professionally unrelated to one another.
- Accounts owned by legal entities pursuing unrelated economic activities, where all accounts are operated by the same individuals.
- Accounts operated through a high number of small credits and a small number of high debits.
- Accounts with frequent credits and/or debits in cash, where such operations are not consistent with the client's profile or business or activity.
- Accounts in which frequent deposits are made by persons apparently personally or professionally unrelated to the relevant accountholders.
- Accounts used to concentrate funds coming from other accounts which are subsequently transferred in block, in particular in the case of outbound international transfers.
- Accounts which, for no apparent reason, evidence a sudden increase in operations, amounts processed and/or their respective average balances.
- Accounts dormant for a long period and which are suddenly operated by significant amounts or deposits in cash.
- Accounts almost exclusively used to transfer funds to and from abroad.
- Accounts owned by entities domiciled in offshore centres and which have the same beneficial owner, with frequent and complex movements of funds.
- Accounts with a high and frequent number of deposits made exclusively through ATMs or night deposit facilities, in particular when these deposits are made in cash.
- Accounts with deposits in cash immediately after their accountholders access a safe that they have in the financial institution.

C. INDICATORS RELATED TO LOANS

- Early repayment of loans, when these are made:
    - unexpectedly and for no apparent logical reason;
    - with economic losses for the borrower;
    - using third-party funds;
    - using funds of uncertain origin and inconsistent with the client's profile;

  - using funds transferred from accounts with several financial institutions; or
  - in cash (in particular in the context of consumer loans).

- Loan applications for no apparent economic reason, taking into account, for instance, the significant value of the assets owned by the client.
- Loan applications by clients who/which show no interest in discussing the terms of the transaction, in particular the costs associated therewith.
- Loan applications based on security or assets, belonging either to the client or a third party, deposited with the financial institution and whose origin is unknown and whose value is inconsistent with the client's financial condition.
- Loan applications by clients who/which have already obtained loans from institutions located in offshore centres and which are unrelated to the client's known business.
- Loan applications by clients who/which declare income whose origin is not fully clarified by its owners to the financial institution.
- Loan applications by clients who/which propose the application of significant sums in deposits or other products in consideration for the approval of such loans.
- Loan applications whose documentation concerning the borrower intended for the respective file is supplied to the financial institution by a third party apparently unrelated to the transaction.
- Absence of evidence of how the sums lent are used, the client withdrawing in cash the loan amount deposited in his/her/its bank deposit account.

D. INDICATORS RELATED TO TRANSFERS OF FUNDS

- Transfers broken down into several transactions, so as to evade compliance with the legal and regulatory obligations applicable to transactions above a certain amount.
- Outbound international transfers inconsistent with the client's known business, notably due to their amount, frequency or beneficiaries.
- Transfers in which – at any time during the fund circuit, including when the funds are made available to their ultimate beneficiaries – any individuals or legal entities not duly authorised to carry out such business by the competent authorities of the relevant countries or jurisdictions act, formally or informally, in any capacity whatsoever.

- Transfers with no apparent connection between the client´s known business and the payors/beneficiaries of the transactions or the countries/geographic areas of origin/destination of such transfers.
- Transfers in which the client refuses or is reluctant to give an explanation for executing the transaction.
- Transfers in favour of a beneficiary or originating from a payor about whom/which the client proves to have little information or is reluctant to supply information.
- Transfers to amounts greater than those foreseeable when the business relationship was established with the client.
- Outbound international transfers to a significant number of beneficiaries apparently without any family ties to the client.
- Transfers to a significant number of beneficiaries who are nationals of countries or jurisdictions publicly known as being related to terrorist activities.
- Transfers regularly instructed by the same individual or legal entity to different beneficiaries and to equal or similar amounts.
- Transfers regularly instructed by the same individual or legal entity to the same beneficiary and to different amounts.
- Transfers instructed by different individuals or legal entities to the same beneficiary, on the same or very close dates.
- Transfers instructed by different individuals or legal entities who/which share one or more personal details (surname, address, employer, telephone number, etc.), and which are executed on the same or very close dates.
- Transfers instructed by different individuals or legal entities whose funds are made available by only one of them.
- Transfers made using third-party funds.
- Transfers to significant amounts with instructions to make the funds available to the relevant beneficiary in cash.
- Inbound international transfers in which the funds transferred are immediately withdrawn from the client's account or, if there is no account, are immediately transferred to other beneficiaries.

- Transfers with instructions to make the funds transferred available to third parties other than the beneficiaries of the transactions.
- Outbound international transfers matched with inbound international transfers to the same or similar amounts.
- Transfers in which clients show unusual interest and curiosity about the fund transfer system, such as operational procedures, limits, etc.
- Outbound international transfers made at a time apparently unrelated to the payment of wages, in particular when instructed by immigrant citizens.

E. INDICATORS RELATED TO MANUAL FOREIGN EXCHANGE TRANSACTIONS

- Transactions broken down into several sales/purchases, so as to evade compliance with the legal and regulatory obligations applicable to transactions above a certain amount.
- Transactions inconsistent with the client's known business, notably due to their amount or frequency.
- Transactions made at a foreign exchange rate more favourable to the financial institution than the advertised rate and/or payment of fees higher than those due, on the client's initiative.
- Transactions in which clients wish to exchange significant sums in a foreign currency for another foreign currency.
- Transactions with non-resident clients who appear to travel to the national territory in order to buy/sell foreign currency.
- Frequent transactions with low denomination banknotes or currencies with low international circulation.
- Transactions in which the clients give instructions to the financial company to subsequently deliver the resulting proceeds to a third party.
- Transactions in which the clients insist upon receiving the proceeds through a cheque of the financial institution, when this is not usual practice in the financial institution in question.
- Transactions in which the clients request to receive the proceeds in foreign currency in banknotes of the highest denomination possible.
- Transactions in which the clients request to receive the proceeds in several postal orders in low amounts, in favour of several beneficiaries.

F. ECONOMIC INDICATORS RELATED TO EMPLOYEES OF FINANCIAL INSTITUTIONS

- Employees who repeatedly fail to comply with AML/CFT legal obligations or internal procedures.
- Employees who establish informal and close relationships with clients that exceed the usual standards applying to their functions or are inconsistent with the financial institution's internal practice.
- Employees who evidence a pattern of social behaviour or other external signs inconsistent with their financial condition as known by the financial institution.

G. OTHER INDICATORS

- Transactions related to the sale of real estate in which:
    - the sale value is significantly above the market value;
    - payment is made by bearer cheque or a cheque endorsed in favour of a third party apparently unrelated to the transaction;
    - payment is made in cash, in particular originating from a bank deposit account owned by a third party apparently unrelated to the buyer; or
    - the property in question has been recently acquired by the seller.
- Transactions related to not-for-profit organisations in which:
- the nature, frequency or amount of transactions is inconsistent with the size of the organisation, its goals and/or its known activity;
- the frequency and amount of transactions suddenly increase;
- the organisation keeps significant amounts in its bank deposit account over extended periods;
- the organisation only obtains contributions from individuals and entities not resident in Portugal;
- the organisation seems to have little, or no human and material means allocated to its activity;
- the representatives of the organisation are not resident in Portugal, in particular when significant sums are transferred to the countries of residence of these representatives; or
- the organisation is somehow related to countries or jurisdictions publicly known as places of production of/trafficking in narcotics, having high levels of corruption, money laundering hubs, sponsors or supporters of terrorism or sponsors or supporters of the proliferation of weapons of mass destruction.

14. ANNEX I

AML/CFT Risk Assessment Methodology of Haitong Bank S.A.

The definition of the AML/CFT risk model should be preceded of an annual risk assessment, and subsequent definition of actions (recurrent tasks and targeted tasks) to undertake within the annual compliance plan (both to be approved by the board of directors) and set forth on the internal framework in compliance with internal control system obligations.

The internal AML risk model should be subject to periodic assessments by the Internal Audit Function and Statutory Auditors, with specific audit works in each of the geographical locations of the Bank with operational activity (Portugal, Brazil, Poland, Spain, Macau and UK).



This AML/CFT risk model applies to Haitong Bank, S.A., its branches and subsidiaries.

i. Current AML Risk model

The Bank's AML/CFT risk model is structured over a mix of policies, regulations and procedures, IT systems and trainings, designed to comply with its lawful obligations given the specificities of the Bank's business activities over its relevant dimensions (i.e., clients and counterparties, types of activities, channels used to engage business relationship, products / transactions, geographies, others specifically identified), as follows:

a) **Policies, Regulations and Procedures:**

- R05 - Anti-Money Laundering and Countering the Financing of Terrorism Regulation;
- PM254 – Account Opening Procedure;
- PM019 - Counterparty Identification Procedure;
- PM029 - Anti-Money Laundering Procedure.

b) IT Systems:

	Standard KYC	AML Scoring	Onboarding screening	KYC search tool	Database filtering	Message filtering	Transaction monitoring
Tool	(MER)	(MER)	LSEG World-Check	dun & bradstreet	FircoSoft	FircoSoft	fiserv.
Scope	Full Database	Full Database	Full Database	Support compliance on company information	Full Database	SWIFT / SEPA / TARGET messages	Transactions
Timing and recurrence	Onboarding, regular updates	Daily, auto	Onboarding, manual	Ad hoc	Weekly, auto	Auto (online) per relevant transaction	Auto (batch) per relevant transaction
Data	Information data and documentation register and archive	KYC data as per the scoring algorithm	Worldwide official and commercial databases on sanctions, embargos, PEP	Consolidates information from hundreds of databases	UN, EU, OFAC and Others (e.g. Bank of Portugal and Bank of England)	UN, EU and OFAC Sanctions	Account and transaction data

* In Brazil: E-Guardian (AML/CFT Transaction Monitoring)

c) Trainings:

- Induction program for newly hired employees.
- AML Annual Training.
- Ad-hoc specialized training attended by Compliance Team

ii. Risk assessment methodology

This risk methodology lists the key assessment factors that the Bank applies to recurrently identify, control and assess the exposure to money laundering and terrorist financing ("**ML-FT**") risks and to analyze the elements of risk which may affect the activities of the Bank, in a view to define, implement and test the effectiveness of its control arrangements and procedures.

The assessment follows a business-unit-focused approach, covering each activity in each geography where the Bank is present and defining the probability and impact levels of the occurrence of events resulting from each of the risk factors considered.
The exercise is reviewed annually, to align the classification used with the one applicable for Bank of Portugal reporting purposes (with a 4-degree scale as follows: low / medium-low / medium-high / high).

The ponderation of all parameters will conduct to a final classification:

- Low Risk: from 0 to 1.49;
- Medium-Low Risk: from 1.5 to 2.25;
- Medium-High: from 2.26 to 3;
- High Risk: above 3.

The weight of each entity in Haitong Bank Group's is calculated based on its contribution to the consolidated assets.

iii. Key inputs for the Risk Assessment

The risk assessment should be made independently by Compliance Department, in particular by the Money Laundering Reporting Officer ("MLRO"), namely by considering the following inputs:

- Specificities of the activities undertaken by each unit and each geography of the Bank as described in Haitong Bank's organizational manual and their procedures manuals;
- Specific knowledge about each transaction undertaken, namely sourced out of Credit and Adoption Committees' materials;
- Data collected in the course of KYC processes escalated to Compliance, including the course of enhanced due diligence processes;
- Review of the KYC database, e.g., change in geography, role, relationship and high risk factors;
- Overall compliance activities over the several units of the Bank;
- Any findings and feedback obtained from authorities in the course of regulatory inspections or other initiatives.

iv. Classification of clients in terms of AML/CFT Risk

Clients are classified as "**High**", "**Medium**" or "**Low**" in line with their inherent risk, according to the Bank's AML Scoring Mechanism, which is duly laid down in this Regulation. This Regulation also lays out the prohibited clients typologies and the rules for accepting Clients.

v. AML/CFT Risk Assessment categories

The General Assessment, each Subsidiary and Branch Assessment and also Unit Assessment are based on the analysis of the level of relevance of a number of risk factors in relation to the following assessment categories ("**Assessment Categories**"):

- Clients / Counterparties;

- Types of Activities;
- Channels Used to Engage Business Relationships;
- Products / Transactions;
- Geographies.

Each risk factor identified below shall be classified as "**High Risk**", "**Medium-High Risk**", "**Medium-Low Risk**" or "**Low Risk**", taking into account the special circumstances of that assessment category. The classification considers facts, opinions, or volumes of activity, as applicable, that are clearly identified.

vi. AML/CFT Risk Assessment factors

Applicable Risk Factors

In order to determine the General Assessment and the Unit Assessments, a selected list of risk factors applicable to each of the assessment categories is rated as "**High Risk**", "**Medium-High Risk**", "**Medium-Low Risk**" or "**Low Risk**".

The risk factors may vary from category to category, as different types of categories have different types of risks associated with them.

In what regards the relationship with Clients / Counterparties, the following risk factors are considered:

- Business relationships that occur in unusual circumstances;
- Legal persons or collective interests' centres without legal personality which are structures of detention of personal assets;
- Companies with fiduciary shareholders (nominee shareholders) or whose capital is represented by bearer shares;
- Clients who pursue activities involving significant operations in cash;
- Customer ownership or control structures which appear to be unusual or overly complex, taking into account the nature of the activity pursued by client;
- Transactions (type, volume) not consistent with customers' expected profile. Behavioural risk is associated with significant departures from the client's standard behaviour and the goals of the client declared upon opening an account and cause a transaction to become suspicious for AML/CFT purposes;
- Involvement with non-profits entities (charities, religious);

- Relationship with PEPs;
- Relationship with persons / entities included in lists of sanctions or restrictive measures;
- Involvement with participants without direct relationship with the Bank;
- Customer volume in respect of retail individuals, high net worth individuals, corporations and institutional clients;
- Percentage of low, medium and high ML risk in terms of client volume.

The risks analyzed in relation to the specific Products / Transactions of the Bank are:

- Private banking (which should be not applicable as the Bank does not provide currently such services);
- Anonymous nature of Products or Transactions;
- Payments received from third parties unknown or not associated with the client or with the activity pursued by the client;
- New products and new business practices, including new delivery mechanisms and payment methods, as well as the use of new technologies or technologies in development for both new and existing products;
- Occasional nature of the business relationship;
- Types of transaction pre-identified as suspicious by the Bank of Portugal;
- The existence of intensive cash transactions (which should be not applicable to the Bank as the Bank does not accepts cash);
- Deviations from the transaction's expectable pattern;
- Existence of banking correspondents domiciled in third countries;
- Association with high-risk sectors (weapons, gambling).

The Channels used to engage clients are also considered for the risk assessment, as the circumstances of communications with clients (face-to-face, anonymity, distance interactions) may increase or mitigate the risk of money laundering.

The risk assessment by Geography covers the countries where the Bank has a presence and which are, as are other assessment categories, in scope for the General Assessment and each Unit Assessment. In this regard, the following levels of exposure are taken into account:

- Countries identified by appropriate sources, such as reports of mutual evaluation, detailed evaluation or monitoring, as lacking effective systems for preventing ML-FT;
- Countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

- Countries or jurisdictions subject to sanctions, embargoes, other restrictive measures or additional countermeasures imposed, inter alia, by the United Nations and the European Union;
- Countries or jurisdictions that provide funding or support for terrorist activities or acts, or in the territory of which terrorist organizations operate.

Scoring Risk Factors

None of the risk factors above is weighed higher than the others. All the risk factors rated as "High Risk", "Medium-High Risk", "Medium-Low Risk" and "Low Risk" are marked as 4, 3, 2 and 1, respectively. The average score of the risk factors within one Assessment Category is the risk level of that Assessment Category.

Further, without taking into account mitigating factors, the average of the risk levels of all Assessment Categories is the level of overall ML/FT risk for Unit Assessments; and the average of the risk levels of all Unit Assessments is the level of overall ML/F risk for General Assessment.

For avoidance of doubt, the scoring of two risk factors under the Assessment Category – Client / Counterpart are particularly elaborate clarified below as they are not simply and directly rated:

a. Client Volume

This risk factor is divided into 4 types of clients: retail individuals, high-net-worth individuals, corporate clients and institutional clients, the number of which in total is the threshold as shown below:

Threshold of Risk Classification of Client Volume:
Low risk: 500 clients in total or below
Medium-low risk: between 501 and 1000 clients
Medium-high risk: between 1001 and 5,000 clients in total
High risk: 5,000 clients or above in total

b. Percentage of Low, Medium and High ML Risk in Terms of Client Volume

The score of this risk factor = (1 x the percentage of client in low ML risk)
(2 x the percentage of client in medium ML risk)
(3 x the percentage of client in high ML risk)

vii. Mitigating factors

Applicable Mitigating Factors

The risk factors assessed as high or medium risk are mitigated by other factors, namely through the various procedures and controls defined for each type of AML risk clients, referred to in the R05 Anti-Money Laundering and Countering the Financing of Terrorism Regulation, thus reducing the ML-FT risk. Although mitigation measures are defined on a case-by-case basis, the following circumstances, actions, or internal procedures typically reduce exposure to ML-FT risks:

- Enhanced KYC/KYT;
- Core transactions of the Bank involve financial and credit review (M&A, ECM-DCM, SF);
- Involvement of third parties with specific obligations in ML/FT prevention (lawyers, consultants);
- Use of dedicated compliance systems over the relevant transaction, including non AML/KYC dedicated systems, such as B-vault (communications surveillance);
- Limited amount of funds handled by Bank;
- No cash deposit service available for clients.

Scoring Mitigating Factors

Where the overall ML/FT risk is at the medium or high level, the averaged mitigating score may be deducted from the overall ML/FT risk to reflect an actual ML/FT risk.

The score of each mitigating factor may be different from the others, depending on its effectiveness of reducing the ML/FT risk. In any case, the score of each mitigating factor must be less than 1 as they are merely performed as compensation for ML/FT risk rather than offsetting the risk.

viii. Outputs of the Risk Assessment

The ponderation of all parameters will conduct to a final classification as "**High Risk**", scored >3; "**Medium-High Risk**", scored >2.25 and ≤ 3; "**Medium-Low Risk**", scored ≥1.5 and ≤ 2.25 and "**Low Risk**", scored <1.5, on the General Assessment and on each of the Unit Assessments.

The risk assessment must take into account specific requirements for each of the Bank's business activities that are subject to AML/CFT legal requirements. A material and descriptive view on the effective actions that should be implemented to address the requirements / improvement opportunities identified, and which should be reviewed and followed up, for example, by updating internal policies,

regulations and procedures, and control systems so that the Bank's business activities are in compliance with AML/CFT regulatory requirements.

ix. Probability and impact of Risk factors

Where applicable, each risk factor identified above should be assigned a probability along with the impact. The criteria behind the probability and impact should be the following:

a. Criteria for the Probability

Probability of Risk Factor	Description
Low	Unlikely to occur
Medium-Low	Likely to occur some times
Medium-High	Likely to occur several times
High	Likely to occur frequently

b. Criteria for the Impact

Severity	Description
Severe	• Revocation/suspension of the authorisation to operate
High	• Sanctions ≥ €1,000,000 • Prevents the Bank from reaching out for new business opportunities and pursuing its expansion • Prevents performance of legal obligations for a medium period of time • Major reputational damage, e.g. public reprimand from authorities/regulators, and negative coverage in the international media • The Bank, or its employees, being subject to legal sanction, criminal offence, civil offence, or proceeding costly litigation • Failing to make prudent, independent reasonable and professional judgement for clients/counterparties
Medium	• Sanctions ≥ €100,000 to < €1,000,000 • Reduces the Bank's ability to reach out for new business opportunities and pursue its expansion in the medium term • Prevents performance of a set of legal obligations for a short period of time • Medium reputational damage, e.g. poor practices revealed by authorities or regulators in their published reports/notice, and negative press coverage in any region • Small regulatory actions, penalties or fines • Failing to make prudent, independent reasonable and professional judgement for general support functions
Low	• Sanctions < €100,000 • Reduces the Bank's ability to reach out for new business opportunities in the short term • Prevents performance of a few legal obligations • Low reputational damage • No regulatory or legal action • Small impact on administrative or secretarial function

Notably, considering that in AML the impact variable is a constant denominator, as AML related infringements potentially applicable by the Bank would follow under articles 170 a) and 171 no. 2, of Law no. 83/2017, notwithstanding the possibility of aggravation as a result of economic benefit (article 171 no. 1 of the same Law) or ancillary sanctions (article 172), the impact dimension is not a relevant variable for measure the degree of exposure of the Bank that will focus on probability for AML risk assessment and risk model definition.

x. Periodic review and update of AML/CFT Risk Assessment

The AML/CFT risk model is reviewed and updated annually or whenever there is any significant change in the activities pursued by the Bank.

The review and update of the risk model take into account the following matters, amongst others:

- Developments in the business and its impact on the activities performed by the Bank;
- Developments in the activities performed;
- The outcome of transactional and behavioural analysis and monitoring;
- Other internal or external factors which might influence the risk assessment.