General principles of VidaCaixa’s Risk Management Policy for the Prevention of Money Laundering and Terrorist Financing and the Management of International Financial Sanctions and Countermeasures

Contents

1. Introduction

1.1 Background

VidaCaixa S.A.U. de Seguros y Reaseguros (hereinafter "VidaCaixa") is firmly committed to the prevention of money laundering and terrorist financing (hereinafter AML/CFT) and compliance with international financial sanctions and countermeasures programmes (hereinafter "Sanctions"), by actively promoting the application of the highest international standards in this area.

Financial crime is a universal and globalized phenomenon that exploits the disappearance of trade barriers and the internationalization of the economy to prosper. Combating this phenomenon requires and demands a coordinated response from the international community in general, and from the financial and insurance sectors in particular, to prevent their inadvertent and unwitting use for illicit purposes.
Furthermore, various national and international bodies have established a series of financial sanctions and/or legal restrictions directed against individuals, entities, and countries for various reasons (violations of international law, human rights, drug trafficking, etc.), and generally involving the freezing of funds and other financial assets, as well as preventing the maintenance of business relationships with these individuals.

Other types of sanctions establish the seizure of certain assets, as well as trade and financial restrictions.

1.2 Concept

Risk of money laundering and terrorist financing prevention and sanctions.

For the purposes of interpreting and applying these Principles, the following definitions shall apply:

Money Laundering (ML):

For the purposes of interpreting and applying this Policy, money laundering is defined as the conversion or transfer of assets derived from criminal activity, in the knowledge that such assets are derived from criminal activity or participation in criminal activity, with the purpose of concealing or disguising their illicit origin or assisting the individuals involved in evading the legal consequences of their actions.

The concealment or disguising of the nature, origin, location, disposition, movement, or actual ownership or rights to assets, in the knowledge that such assets are derived from criminal activity or participation in criminal activity.

The acquisition, possession, or use of such assets, in the knowledge that at the time of receipt they are derived from criminal activity or participation in criminal activity.

Participation in any of the activities mentioned in the preceding paragraphs, association to commit such acts, the attempt to perpetrate them, and the act of helping, instigating, or advising someone to carry them out or facilitating their execution.

All types of assets—tangible or intangible, movable or immovable—whose acquisition or possession originates from a crime are considered proceeds of criminal activity. This also includes documents or legal instruments, regardless of their form, including electronic or digital, that prove ownership or a right to the aforementioned assets. Furthermore, the amount defrauded in the case of tax offenses is also included.

Money laundering is understood to have occurred even if the activities that generated the assets took place in the territory of another State.

Finally, it should be noted that the following phases are typically distinguished in the money laundering process:

- **Placement or concealment:** Introduction of cash from criminal activities into financial systems or conversion to a different asset.
- **Accumulation:** Transferring or moving funds between different products or services in one or more jurisdictions in order to divide, accumulate, conceal, transfer, and deposit them in jurisdictions with less stringent investigations into the origin of wealth, or in accounts where the money appears legitimate, or carrying out other transactions that prevent the true origin of such monies to be traced.
- **Integration:** Incorporating capital into the financial system under the guise of legitimacy.

VidaCaixa can be used at any stage of the described process, primarily at the "placement" stage, so the necessary internal control measures must be adopted in order to manage this risk.

Terrorist Financing (TF)

Terrorist financing is defined as the supply, deposit, distribution, or collection of funds or assets, by any means, directly or indirectly, with the intention of using them or with the knowledge that they will be used, in whole or in part, for the commission of any of the terrorist offenses defined in applicable criminal law.

Terrorist financing will be considered to exist even if the supply or collection of funds or assets takes place in the territory of another State.

Current regulations on the prevention of money laundering also include certain obligations regarding international financial sanctions; therefore, the management of the risk arising from these will also be addressed in this Policy.

International Financial Sanctions and Countermeasures (Sanctions)

Financial sanctions are a set of regulations, both national and international, issued by various bodies to impose, among other things, international measures against specific jurisdictions, concrete actions against individuals or organizations involved in terrorism, drug trafficking, the proliferation of weapons of mass destruction, threats to national or international security, etc.

The objective of these sanctions and restrictive measures is to:

- Prohibit the establishment of commercial relations with certain individuals or entities
- Restrict or prohibit economic and commercial activities with certain individuals and legal entities
- Restrict or prohibit transactions with certain jurisdictions.

These sanctions may be directed against specific jurisdictions or against specific individuals or legal entities:

✓ **Jurisdictions.** The Programmes may establish:
  o Total or partial restrictions
  o Embargoes on certain goods (weapons, precious metals, raw materials, etc.)
  o Restrictions on sectors of economic activity, on the provision of services,

✓ **Individuals.** The Programmes may establish:
  o Prohibitions on establishing commercial relationships with certain individuals
  o Financial restrictions, which may require the mandatory freezing of all funds and economic resources belonging to the sanctioned individuals and entities, as well as the prohibition of making funds or economic resources available to the aforementioned individuals and entities, directly or indirectly, or for their benefit.

1.3 Objective

The purpose of this document is to develop for VidaCaixa the principles and premises that regulate the risk of money laundering and terrorist financing (hereinafter ML/TF) and sanctions.

The purpose of these VidaCaixa General Principles of the Risk Management Policy for the Prevention of Money Laundering and Terrorist Financing and Management of International Financial Sanctions and Countermeasures (hereinafter the "Principles") is to establish a compliance framework, which must be applied in the exercise of its activities, business and relationships, both nationally and internationally, in order to prevent money laundering and terrorist financing and comply with the different programmes of international financial sanctions and countermeasures that may be applicable.

2. Scope of application

These Principles apply to VidaCaixa as a whole (all employees and managers of VidaCaixa)

Business units assigned prevention and supervision functions will develop their respective rules and/or procedures for their correct implementation, execution and compliance.

The governing bodies of VidaCaixa will adopt the appropriate decisions in order to integrate the provisions of the Corporate Policy following the principle of proportionality, the governance framework for the specificities of their structure of governing bodies, committees and departments, and their principles of action, methodologies and processes.

This integration involves the approval of VidaCaixa's own policy, including the principles and premises of the Corporate Policy, and its adaptation to the specificities and risks of the insurance sector.

3. Regulatory framework. Regulations and applicable standards

This Policy will be governed by the provisions of the current applicable regulations, as well as by any that modify or replace these in the future. Specifically, as of the date of its drafting, the applicable legislation for VidaCaixa is as follows:

- Law 10/2010, of 28 April, on the prevention of money laundering and terrorist financing.
- Spanish Royal Decree 304/2014, of 5 May, passing the Regulations for Law 10/2010.
- Spanish Royal Decree 413/2015 of 29 May, passing the Regulations of the Commission for Monitoring Terrorism Financing Activities.
- Law 12/2003, of 21 May, blocking the financing of terrorism.
- European Union regulations related to the application of anti-money laundering legislation.
- Regulation (EU) 2024/1624 of the European Parliament and Council, of 31 May 2024, relating to the prevention of the use of the financial system for money laundering or financing of terrorism.
- Regulation (EU) 2024/1620 of the European Parliament and Council, of 31 May 2024, creating the Authority to Combat Money Laundering and Terrorist Financing and amending Regulations (EU) No. 1093/2010, (EU) No. 1094/2010 and (EU) No. 1095/2010.
- European Union regulations related to the application of international financial sanctions.
- Standards of international bodies, primarily represented by the Recommendations of the Financial Action Task Force (FATF).
- EBA guidelines on policies and procedures relating to compliance management and the role and responsibilities of the AML/CFT Officer under Article 8 of Directive (EU) 2015/849 (EBA/GL/2022/05 - 14 June 2022).

4. Management Framework for AML/CFT and Sanctions

A. ADMISSION POLICY AND DUE DILIGENCE MEASURES

1. Customer Admission

1.1 Introduction

In compliance with AML/CFT regulations, at the CaixaBank Group level, a customer onboarding policy has been developed that includes a classification of different customer types, and the identification of those who may potentially pose a higher-than-average risk, either due to regulatory requirements or as determined by an internal risk analysis. This customer onboarding policy will be phased in, with enhanced precautions being taken for customers who present a higher-than-average risk. The policy includes measures to mitigate this risk, which may include, where applicable, refusing to establish business relationships, execute transactions, or terminating existing business relationships.

VidaCaixa's customer admission policy is aligned with that of CaixaBank (included within CaixaBank's Corporate Policy for the Prevention of Money Laundering and Terrorist Financing). It states that several factors have been taken into account to determine the risk level of customers:

- Customer characteristics:
  - Activity
  - Geographic area
  - Politically Exposed Person (PEP)
  - Identity of the Beneficial Owner
  - Ownership or control structure

- . Product characteristics:
  - Product type
  - Business segment
  - Relationship channel

- . Operation features:
  - Source of funds
  - Transactions

1.2 Customer classification

In accordance with the criteria described in the previous section, the following customer categories are established based on their ML/TF risk:

Individuals or entities excluded from admission

For reasons of money laundering and terrorist financing risk control, the following natural or legal persons will not be accepted as customers, nor will business relationships be established with them (in the case of legal persons, those whose beneficial owner or director falls under any of the following categories will also not be accepted):

Individuals to whom, during their admission process, the due diligence measures provided for in this Policy could not be applied.

- Individuals included on international sanctions lists and other official lists, and individuals included on public lists related to terrorism, affiliated groups, or organized crime.
- Persons included on international sanctions lists and other official lists and persons included on public lists related to terrorism, affiliated groups or organized crime. For these purposes, the lists that Caixabank has implemented shall apply at all times.
- People or entities that should not be admitted as customers in accordance with the Group's International Financial Sanctions Policy and applicable legal regulations.
- People whose businesses are of a nature that makes it impossible to verify the legitimacy of the transactions or the source of the funds.
- People who refuse to provide documentation that allows for full formal identification of the beneficial owner or, having provided such documentation, refuse to allow the Entity to retain a digital copy thereof.
- People who provide manifestly false documents or documents that raise serious doubts about their legality, legitimacy, or lack of manipulation, or that do not offer sufficient guarantees.
- People who refuse to provide required information or documentation relating to the verification of the declared activities or the source of the funds, as well as information regarding the purpose and nature of the business relationship with the Entity.
- People and legal instruments whose ownership or control structure cannot be determined, or companies whose beneficial owner cannot be determined.

- Shell banks and financial institutions that operate with these types of entities.
- Individuals or entities intending to carry out operations related to financial activities, gambling, betting, payment services, currency exchange, issuance or intermediation of cryptocurrencies or crypto assets, or other activities without the respective official authorization or other legally required qualifications.
- Any other category not included above that may be rejected based on legal regulations or the Entity's internal policy.
- Natural or legal persons who, having previously been customers of the entity, have ceased to be so pursuant to this Policy and CaixaBank Group's Corporate Policy on the Prevention of Money Laundering and the Financing of Terrorism and the management of international Financial Sanctions and Countermeasures.

High-Risk Individuals or Entities

All individuals included in this category shall be considered high-risk for AML/CFT purposes and be subject to the enhanced due diligence measures provided for in this Policy, requiring in all cases the authorization of the relevant business department director and subsequent ratification by the Operational Department for the Prevention of Money Laundering.

The following are included as high-risk individuals or entities:

- Natural persons, whether national or foreign, who are politically exposed persons (PEPs).
- Legal entities, whether national or foreign, whose beneficial owner is a politically exposed person (PEP), whether national or foreign.
- Natural persons residing in a high-risk jurisdiction.
- Legal entities domiciled in a high-risk jurisdiction, or, if domiciled in a country other than those considered high-risk jurisdictions, whose beneficial owner by ownership or control resides in a high-risk jurisdiction.
- Individuals or entities whose activity consists of the issuance or intermediation of “cryptocurrencies” or “crypto-assets” in general.
- Customers related to the production, marketing, distribution and sale of weapons and other military items.
- Electronic money institutions and payment institutions when they carry out money transfer or foreign currency exchange activities.
- Casinos, companies operating recreational games, and other companies linked to gambling that have the respective official authorization or other legally required qualifications, as well as any other high-risk sector when required by their specific procedures.
- Companies with bearer securities, once their ownership or control structure has been determined.
- Any natural or legal person whose characteristics or operations lead the Operational Department for the Prevention of Money Laundering to conclude that it is advisable to submit their acceptance as a customer or their risk classification to its own consideration; in particular, those persons with adverse reports related to money laundering operations, those convicted of economic crimes, etc.
- Mere Asset Holding Entities (META)

All other individuals or entities shall be subject to standard or simplified due diligence measures as established by applicable regulations or internal rules and procedures.

Formal Customer Identification.

The rules and procedures implementing these Principles must guarantee the proper identification of all customers within the Group companies, in accordance with applicable legislation at any given time and in each jurisdiction. This will include, in all cases, verification of identity through valid and current documents.

Under no circumstances shall business relationships be maintained with individuals who cannot be identified. Furthermore, the contracting of anonymous, encrypted, or fictitious products or services is prohibited. Prior to establishing business relationships or executing transactions, the beneficial owner must be identified. This obligation implies that, if there are indications or certainty that customers are not acting on their own behalf, precise information must be obtained in order to ascertain the identity of the individuals on whose behalf they are acting. Furthermore, sufficient documentation proving the authority under which they are acting.

Knowledge of the customer's business and assets.

Prior to the establishment of a business relationship, VidaCaixa must collect, at least, information about the customer's professional or business activity and the origin of the funds or assets. Depending on the risk level assigned to the customer, additional measures may be taken, including documentary verification and verification through reliable external sources of the information provided by the customer, particularly regarding their professional or business activity, the origin of funds or assets, and any other relevant information, in accordance with internal rules and procedures.

B. DETECTION, CONTROL, AND REVIEW OF SUSPICIOUS TRANSACTIONS

VidaCaixa must have resources for the detection, control, and examination of transactions. These resources will be applied according to risk and will, in all cases, include the three basic methods for detecting transactions:

a. Internal reports of suspicious activity by the entity's employees.

b. Detection of potentially suspicious transactions through established alert systems.

c. Reports from supervisory bodies or law enforcement or judicial authorities.

The detection of suspicious transactions will entail a detailed and comprehensive analysis aimed at determining the actual existence of evidence of money laundering and terrorist financing.

C. COMMUNICATION OF OPERATIONS AND OTHER RULES OF ACTION

VidaCaixa will, on its own initiative, report to supervisory and/or financial intelligence agencies any fact or transaction, including mere attempts, that, once a special examination is completed, reveals evidence or certainty of a connection to money laundering or terrorist financing. In particular, transactions that show a clear lack of correspondence with the nature, volume of activity, or operational history of the customers shall be reported to the supervisory agencies.

The decision to report shall be made centrally in each jurisdiction by the persons or bodies designated for this purpose and carried out through the authorized representative before the competent authorities. The report shall, in all cases, include information on the decision regarding the continuation or discontinuation of the business relationship, as well as the justification for this decision. Notwithstanding reporting based on evidence, the entity shall immediately adopt additional risk management and mitigation measures that must take into account the risk of disclosure.

Employees must refrain from carrying out any operation for which there is any indication or certainty that it is related to money laundering or the financing of terrorism.

Employees and managers shall not disclose to the customer or to third parties that information has been communicated to internal control bodies or the supervisory body, or that any transaction is being or may be examined as to whether it could be related to money laundering or the financing of terrorism.

D. MANAGEMENT OF INTERNATIONAL FINANCIAL SANCTIONS

For compliance with the restrictions imposed by the Sanctions programmes, VidaCaixa must:

- Identify and monitor the sanctions programmes established by the United Nations (UN), the European Union (EU), OFAC, and local programmes applicable in the jurisdictions in which it operates.
- Assess the risks associated with activities related to sanctions programmes in order to determine the risks of participating or engaging in activities restricted or prohibited by the sanctions. Refrain from executing or participating in operations or transactions with sanctioned individuals.
- Comply with prohibitions and restrictions on the execution of transactions, payments, or business relationships and refrain from executing them when they would violate the sanctions programmes.
- Freeze assets and funds when required by the sanctions programmes and report such action to the authorities administering the sanctions programmes.
- Implement internal control procedures and prevention mechanisms that allow for proper compliance with obligations, including automated screening procedures and tools.

E. DOCUMENT PRESERVATION

VidaCaixa will retain, for a minimum period of ten years (starting from the termination of the business relationship or the execution of the transaction), the documentation formalizing compliance with the obligations established in current regulations. In particular, it will retain, for use in any investigation or analysis regarding potential prevention cases by supervisors or any other competent authority:

- Copies of the documents required for due diligence measures, including, in particular, copies of authentic identification documents, customer declarations, and documentation and information provided by the customer or obtained from reliable independent sources.
- Original or legally valid copies of documents or records that adequately prove the transactions, parties involved, and business relationships.
- Regarding sanctions, documents supporting the management of incidents, the decisions made by each body, and their eventual communication to the authorities.
- Copies of specific or general sanctions licenses submitted by customers.

Five years after the termination of the business relationship or the execution of the occasional transaction, the retained documentation shall only be accessible to VidaCaixa's internal control bodies.

For such purposes, VidaCaixa shall have a document repository for the preservation of documentation in electronic format.

In addition, and in accordance with current legislation, VidaCaixa must retain all documentation formalizing compliance with its communication and internal control obligations:

- Communication with supervisory bodies.
- Notification of the appointment of representatives to the Financial Intelligence authorities.
- Special examination files.
- Information requests and traceability requests received from supervisory bodies.
- Annual reports of external expert examinations and related documents.
- Minutes of meetings of internal control bodies, as well as minutes and documents from other bodies regarding matters with an impact on prevention.

F. STAFF TRAINING

1. Training Plans

Ongoing employee training in the area of anti-money laundering and counter-terrorist financing is one of the cornerstones of the effectiveness of the AML/CFT Policy.

A comprehensive AML/CFT Training Plan will be implemented in order to ensure an adequate level of awareness among all staff, and its content shall be permanently available to all employees. This Plan shall be mandatory for all staff (including Senior Management and the Board of Directors) and must be applied upon the hiring of new employees.

In addition, VidaCaixa must establish an Annual Training Plan with the specific activities to be carried out each year.

VidaCaixa's Human Resources Department will be developed jointly with the Operational Department for the Prevention of Money Laundering, with the aim of:

- Providing adequate training on detecting suspicious transactions and communicating the procedures to follow in such cases.
- Providing specific training on this subject to personnel in all VidaCaixa's business areas that are directly involved in AML/CFT.
- Achieving the ultimate goal of a corporate culture in this area.

2. Training Activity Record

The Human Resources Department shall be responsible for implementing the Training Plan, scheduling training sessions, and managing their proper registration in order to ensure that they are duly accredited, as well as documenting the level of training completion annually.

The Operational Department for the Prevention of Money Laundering shall inform the Group's Internal Control Office (ICO) periodically, and at least once a year, of the level of compliance with the training plan.

G. CONSOLIDATED RISK MANAGEMENT

Caixabank believes that the best way to combat the risks associated with these Principles is through their consolidated management and the uniform and aggregated management of information related to these risks by the Group, regardless of the jurisdiction in which the member companies operate.

The principle of aggregated or consolidated management thus becomes a fundamental pillar of the prevention model and allows for the uniform coordination of efforts across all Group companies, as well as the aggregated assessment and management of risks.

Therefore, all companies that make up the Group shall keep Caixabank promptly informed about high-risk relationships, data on sensitive activities and their associated risks, and promptly respond to any request for information that Caixabank may make in the management of regulatory and reputational risk related to money laundering, terrorist financing and sanctions.

These obligations are understood notwithstanding strict compliance with applicable regulations, and especially with data protection and privacy. Caixabank and the Group companies shall take the necessary measures to preserve the confidentiality and privacy of the data communicated between Group companies.