GENERAL PRINCIPLES OF CAIXABANK's CORPORATE POLICY ON COMPLIANCE

July 2021

CONTENTS

1. Introduction

1.1 Background

There are several regulatory provisions of different levels that require organisations to set up a specific division to perform the function of Compliance and to promote corporate ethical principles, thus reaffirming a rule of law corporate culture and regularly verifying and evaluating the efficiency of the controls related to the risk of non-compliance with the associated obligations.

Within this framework for action, the CaixaBank´s Board of Directors approves this CaixaBank's Corporate Policy on Compliance ("the Policy").

1.2 Persons subject to this Policy

Regulatory Compliance is the responsibility of each member of the organisation; this responsibility is distributed as follows regarding the Compliance function and employees:

a) Compliance Function

The main responsibilities of the Compliance Function are as follows:

- To define, implementing and maintaining a **Compliance Programme** that guarantees the correct and efficient implementation of the Compliance Function.
- Continuously identifying, monitoring and assessing **compliance risk**.
- To ensure that the **Governing Bodies and Senior Management** of the Bank are **informed** regarding the most relevant aspects of Compliance and the actions plans to address any weaknesses.
- **Aiding** and **advising** the **Senior Management** and all other CaixaBank's personnel and its subsidiaries on adequately managing compliance risk.
- **To promote, coordinate, monitor and, if applicable, implement training plans within the scope of Compliance** for the Bank's employees.
- Maintaining permanent **contact** with the **main regulators and supervisors** in order to be aware of their expectations and help maintain a fluid communication which involves keeping them apprised of CaixaBank's main regulatory initiatives and projects.
- Leading, together with the areas responsible for Corporate Social Responsibility, the process for disseminating the **values** and **principles enshrined in CaixaBank's Code of Ethics**.
- Planning and following up, with a risk-based approach, the key activities to be carried out by the Compliance Function during the year. This plan is provided in the **Annual Compliance Plan**.
- Promoting a culture of compliance with the rules within the Organisation, promoting the establishment and maintenance of an **adequate governance framework** that

facilitates compliance, throughout the organisation, of the regulations, policies, procedures and standards of conduct.

b) Employees

The principal obligation of all CaixaBank's employees is **to be aware of and comply** with the internal and external regulations, guidelines and instructions laid down by the Governing Body, the Senior Management and the Compliance Function during their daily activities.

Likewise, according to the contents of CaixaBank's Code of Ethics, it bears repeating that all employees have a duty to **inform**, and where applicable, **report** any type of non-compliance with the regulations or ethical standards of which they have knowledge via the Reporting and Whistleblowing Channel.

CaixaBank expressly prohibits and will not tolerate reprisals against individuals reporting a possible breach, or against those helping/involved in the investigation, provided they have acted in good faith and played no part in the reported event. CaixaBank shall adopt appropriate measures to guarantee the protection of the whistle-blower.

1.3 Objective

The mission of the Compliance Function is to identify, evaluate, supervise and report on the risks of sanctions or financial losses to which the Bank is exposed, as a result of the breach or defective of compliance with laws, regulations, legal or administrative requirements, codes of conduct, ethical standards or good practices, relating to the scope of action and in reference to the legal/regulatory and conduct risks (compliance risk); as well as to advise, inform and assist the senior management and the Governing Bodies in relation to compliance, promoting a culture of compliance in the form of training actions, information and awareness throughout the entire organisation

For this purpose, the mission of Compliance is expressed through the following objectives:

- **Supervising the compliance risk** arising from the processes and activities carried out by the company.
- **Promoting the corporate values and principles enshrined in the Code of Ethics** and that guide the Bank's actions.
- **Promoting a culture of control and compliance with the laws and legislation in force** (both external and internal) that permit and favour their integration into the management of the whole organisation.

The contents of this Policy include:

- General strategy or principles that govern compliance risk management

- Governance framework
- General aspects of compliance risk management
- Control framework
- Reporting/information framework

2. Scope

This is a corporate-level policy. Therefore, the principles of activity defined within it apply to all CaixaBank's Group companies that carry out any activity exposed to compliance risk. The Governing Bodies of these companies will make the decisions necessary to integrate the provisions of this Policy. They will apply the principle of proportionality to adapt the governance framework to the idiosyncrasy of their structure of Governing Bodies, committees and departments, and their principles of action, methodologies and processes to the contents of this document.

This integration process may require the subsidiaries to approve their own policies, among other decisions. Approval will be necessary at subsidiaries that need to adapt the contents of this Policy to their own specific characteristics, whether due to the nature, jurisdiction or materiality of the risk at the subsidiary. In this case, CaixaBank's Compliance Function or the corresponding committee, provided that its functions are recognised as corporate in nature, will ensure the alignment of these policies with the corporate policy and their consistent application throughout the CaixaBank Group.

Where risk control and management activities at the subsidiary are carried out directly by CaixaBank, whether due to the materiality of the risk at the subsidiary, for reasons of efficiency, or because the subsidiary has outsourced the operational management of this risk to CaixaBank, the Governing Bodies of the affected subsidiaries shall be informed of the existence of this Corporate Policy and its application to such subsidiaries.

Aside from being a corporate policy, this Policy is also the individual policy of CaixaBank S.A., the parent of the CaixaBank Group.

3. Regulatory framework. Applicable standards and regulations

This Policy shall always be governed by the pertinent legislation in force and any legislation amending or replacing it in the future. At the date of this document the pertinent regulations applicable to the Compliance Function are as follows:

- **US Foreign Corrupt Practices Act** (FCPA), 1977
- Enterprise Risk Management - Integrated Framework (**COSO I**, 1992)
- OECD Anti-Bribery/Corruption Convention (1997) – **Convention on Combating Bribery of Foreign Public Officials in International Business Transactions**
- **The OECD Principles of Corporate Governance** (1999)
- The UN Convention against **Corruption** (2003)
- Business Principles for Countering **bribery.** International transparency (2003)
- Australian Standard on **Compliance Programs** – 3806-2006 (2006)
- **Compliance and the Compliance function in Banks** (Basel Committee on Banking Supervision, 2005)
- Enterprise Risk Management – Integrated Framework" (**COSO II**, 2004)
- **Criminal Code** Reform OL 5/2010 (2010)
- **UK Bribery Act** (2010)
- Guidance to the US FCPA (2012) – Resource Guide and compilation of information
- Guidelines on **Internal Governance** (EBA GL 44)
- CNMV Circular 1/2014 of 26 February on the internal organisational requirements and the **control functions** of institutions that provide investment services
- **Criminal Code** Reform OL 1/2015 (2015)
- **Corporate Governance Principles for Banks** (Basel Committee on Banking Supervision, 2015)
- G20/OECD Principles of Corporate Governance (2016)
- Spanish Circular 1/2016 of the Public Prosecution Service on the **criminal liability of legal entities** following the reform of the Criminal Code by OL 1/2015 (2016)
- ISO 37001 Standard – **Anti-Bribery** Management Systems (2016)
- UNE 19601 Standard – **Criminal Compliance** Management Systems (2017)
- Guidance on "COSO Enterprise Risk Management – Integrating with Strategy and Performance" (**COSO III** ERM, 2017)
- EBA Guidelines of 30 June 2018 on **Internal Governance** – EBA/GL/2017/11 (2017)
- ISO 37301 Standard – **Compliance** Management Systems
- **Final Guidelines on the compliance function under** MiFID II – ESMA35-36-1952
- Directive on the **protection of persons who report** breaches of Union law (2019)
- **CNMC Guide** on Compliance programmes in relation to **Antitrust Principles**

Where subsidiaries are subject to foreign jurisdictions or supplementary sector regulations, the policies and procedures that these subsidiaries roll out shall, in addition to their own standards, take into account the consolidated obligations contained in the aforementioned regulations wherever they do not contradict the specific requirements of the corresponding jurisdiction or sector regulations.

Finally, the necessary standards, guides or procedures for correct implementation, execution and compliance with this Policy shall be implemented at each Group company.

4. General principles of the Compliance Function

With the aim of performing the mission undertaken by the Governance Body, Compliance carries out its function in line with the following principles:

a) Autonomy

The Compliance Function is an autonomous function, which means that it will have sufficient initiative to carry out its functions, without the need to receive specific instructions from other areas or act on their behalf.

The Compliance Function must have sufficient autonomy to make decisions without the need for another area or function of the organisation to approve or authorise its opinions.

b) Independence

In order to guarantee the objectivity of its decisions, the Compliance Function will operate under the principal of functional independence with regard to those areas or functions over which the supervision and monitoring of compliance risk is carried out.

In order to guarantee its independence, the Compliance Function will not be subject to the fulfilment of commercial objectives and will be subject to solely those relating to its activity and the Bank's overall corporate goals.

The competent Governing Bodies will be responsible for appointing and removing its members and establishing their remuneration (both fixed and variable and the proportion between both, respecting the principle of reasonableness at all times). The Governing Bodies shall also assess the degree of achievement of its objectives or goals, subject to compliance with prevailing legal requirements.

No person performing Compliance Functions may be involved in providing the services and activities that they control so as to avoid any undue influence in performing those functions.

The Compliance Function will in all cases have direct access to the Management and Governing Bodies when performing its duties and responsibilities.

c) Authority

The Compliance Function will at all times be positioned at the highest hierarchical level of the Organisation (Senior Management) and shall have sufficient authority so that its lines of action and decisions are assumed by other areas of the entity.

The Compliance Function will, at any time, be able to initiate evaluation and/or verification processes or investigations relating to the areas or processes that expose the Bank to real or potential risks of non-compliance.

d) Human and technical resources

Due to the importance of the mission of the Compliance Function and its responsibilities within the organisation, the areas that carry out the Compliance Function must have sufficient resources to undertake the activities and responsibilities assigned to the Compliance Function in this policy.

They must therefore be allocated sufficient material, IT and technical resources so that Compliance may effectively carry out its function taking into account the nature, volume and complexity of the operations and the nature of the risks assumed by the Bank.

To this end, the Compliance Function must have a budget that allows it to carry out its activities. This budget must be according the level of risk of non-compliance to which the Bank is exposed.

e) Aptitude and integrity

All persons carrying out the Compliance Function will have the necessary knowledge, experience, qualifications and professional integrity to be able to properly carry out their duties throughout the organisation and thus guarantee an extensive and permanent coverage of the Compliance Function.

To this end, training programs and certification plans must be established for those employees assigned to carry out the Compliance Function, as well as plans to enable their professional development.

f) Access to information

The Compliance Function will have access to as much information and documentation as deemed necessary to adequately carry out its functions; it shall also have the necessary assistance at all levels to respond in due course to requests for information received from the supervisory bodies.

g) Risk-based approach

In the performance of its activity, all areas involved in regulatory compliance, and in particular the Compliance Function, must at all times apply a risk-based approach, and therefore carry out a continuous evaluation of the compliance risk associated with the main processes, to prioritise the supervisory and monitoring activities ascribed to the Function, as well as appropriately allocate the resources according to the risks identified.

h) Permanence

In order to carry out the mission and tasks entrusted to it by prevailing legislation, the Compliance Function must exist and form part of the Bank's organisational structure at all times, regardless of the specific persons attached to the function.

5. Management model for the Compliance Function

5.1 Management model

The Management model of the Compliance Function has two main pillars:

a) Risk taxonomy for Compliance
b) Definition of the scope of the Compliance Function within the control environment: Three lines of defence model

5.1.1 Risk taxonomy for Compliance

The risk taxonomy for Compliance is a classification by categories of the compliance risk to which the Bank is exposed, based on the general catalogue of risks of the CaixaBank Group.

The Risk Compliance division permits the scope of the actions of the Compliance Function to be more easily defined into different categories, and represents the starting point for the ongoing evaluation of compliance risks.

It also serves as a basis for identifying and prioritising the activities on which the Compliance Function must focus during the year (Annual Compliance Plan), for updating the GAP list (compliance weaknesses and deficiencies) and for implementing the initiatives and projects of the Compliance area.

In accordance with CaixaBank's Internal Control Policy, Compliance is responsible for supervising the following risks, from among those detailed in the Corporate Risks Catalogue:

- Conduct
- Legal and Regulatory

The subcategories that make up this Compliance Risk Taxonomy are subject to annual review by the Global Risk Committee.

5.1.2. Definition of the scope of the Compliance Function within the control environment: Three lines of defence model

As part of the global risk management model at corporate level and of the Governance and Internal Control policies of CaixaBank, the Compliance Function supervises and manages the compliance risk already identified in the taxonomy of corporate risks, following the three lines of defence model, in which the functions and responsibilities of each defence line are defined.

The Compliance Function exercises its supervisory function from the second line of defence, and in accordance with the Internal Control Policy, identifies, measures, defines and monitors the compliance risk appetite, and is responsible for the independent review of the application of the policies and procedures by the first line of defence. The Compliance Function acts independently from the business units, ensuring the existence of policies for the management and control of compliance risk, monitoring its application, evaluating the control environment and reporting all material risks.

5.2 Key elements of the Compliance Function

The Compliance Function relies on the following key elements to ensure adequate coverage of compliance risk:

- Compliance Programme
- Annual Compliance Plan
- GAP process

5.2.1 Compliance Programme

The Compliance Programme is a set of processes and activities that organise and systematise the main activities of the Compliance Function by following a methodology that is generally accepted worldwide.

The application of the Compliance Programme is based on the execution of a series of key activities, including:

5.2.1.1 Policies on Regulatory Compliance

A crucial element of the CaixaBank's Compliance Programme is the creation and maintenance of Compliance Policies, which clearly establish the requirements and criteria that the Bank must follow with regard to compliance risk.

5.2.1.2. Identification and implementation of regulatory and legislative changes

This involves the preparation and effective implantation and monitoring of a regulatory implementation protocol that enables the identification of regulatory and legislative changes and new developments that affect the Bank in terms of compliance risk, as well as the analysis of the impact that this may have on the Bank's processes and activities.

5.2.1.3 Risk map and indicators

This refers to the creation and maintenance of an inventory of key regulations that affect CaixaBank's activity and which are associated with the taxonomy of compliance risks, as well as the identification, implementation and monitoring of indicators to monitor, detect and mitigate these risks.

5.2.1.4 Advisory services

As previously described, the Compliance Function is entrusted with the crucial task of providing advice to the Governing Bodies and Senior Management and the rest of the organisation on all relevant aspects related to the mission of Compliance. When carrying out this function, the Compliance Function must have, where applicable, the support of the other specialised departments within the Bank, depending on the matter at hand.

5.2.1.5 Regular assessment of compliance risk

One of the key elements of the Bank's Compliance Programme is the regular performance of the compliance risk assessment, as a means of prioritising the activities to be carried out by the Compliance Function and to determine the criticality of those activities and allocate resources accordingly.

The compliance risk assessment must take into account the risk inherent in the activity, together with the result of the supervision of the control environment, the conclusions reached by the internal and external audits and supervisory bodies, and the activity carried out by Customer Service and also the queries or disclosures submitted via the appropriate channel for such purpose and for which the Compliance Function is responsible for processing.

5.2.1.6 Monitoring and testing

The Compliance Function relies on monitoring and testing techniques to evaluate the control environment associated with compliance risk, with a risk-based focus.

This control involves the ongoing monitoring and review of activities based on key risk indicators (KRIs) or internal decisions for the early detection of deviations or improper actions arising from non-compliance with regulations.

Testing consists of the validation of the regulations associated with compliance risk in the Bank's day-to-day processes, through independent verification techniques such as sampling, process reviews, or any other type of test.

5.2.1.7 Training and awareness

In order to comply with the mission with which it has been entrusted, the Compliance Function implements an ongoing range of programmes for training, communication and awareness-raising for the entire workforce so as to promote a culture of compliance and awareness of the obligations and responsibilities of Compliance. These actions will be detailed in the Annual Training Plan to be implemented in close collaboration with Human Resources.

5.2.1.8 Communication and Information (Reporting)

The Compliance Function must favour an appropriate governance framework for recording and reporting, in a timely and efficient manner, to the Bank's Governing Bodies, any significant control weakness related to compliance risk.

5.2.2 Annual Compliance Plan

The Annual Compliance Plan contains a list of activities of the Compliance Function during the reference period (calendar year), together with a schedule for its implementation, all with the aim of guaranteeing that the activities exposed to risk are regularly reviewed, evaluated and communicated.

The principle of proportionality and a risk-based approach will be applied when defining and prioritising the Plan so that the key activities to be carried out during the year can be generated and planned accordingly, depending on the results of the risk assessment, the risks previously identified and the forecast supervisory actions.

The Annual Compliance Plan will be monitored periodically in order to inform the Management and Governing Bodies of the Plan's main conclusions, the degree of implementation with regard to the initial planning and the most significant changes that may have arisen.

5.2.3 GAP process

The GAP process is the key element that the Compliance Function relies on discharging its function as the second line of defence over compliance risks and reporting to Senior Management.

A Compliance GAP means any identified weakness in the control environment associated with compliance risk, resulting in:

- Non-compliance with legislation or current regulations in relation to the risks managed by the Compliance Function
- Business practices carried out by the Bank and/or its employees that are inappropriate or contrary to the Code of Ethics and applicable legislation

GAPs may arise from the implementation of any of the activities that make up the Compliance Programme and which are normally reflected in the Annual Compliance Plan, as well as those inspections carried out by the supervisors and the internal and external auditors in which deficiencies in the control environment are identified.