General Principles of the Regulatory Compliance Policy

20 February 2025

Contents

1. Introduction

1.1 Background

There are various regulatory provisions of varying importance that require organisations to have a specific function tasked with regulatory compliance (hereinafter "Regulatory Compliance" or "*Compliance*"), promoting corporate ethical principles, entrenching a corporate culture of absolute respect for the law, and regularly verifying and evaluating the efficiency of the controls in place in relation to the risk of non-compliance with all related obligations.

Within this framework of action, the Board of Directors of Caixabank, S.A. ("CaixaBank" or "the Bank") hereby approves this Corporate Regulatory Compliance Policy ("the Policy").

1.2 Scope

In such a scenario, it is essential to have a Compliance Function within the Bank and to ensure that it has an organisational and management model that complies with the applicable regulations and with the highest national and international standards.

Compliance is the responsibility of each and every member of the organisation, i.e. all employees, managers and members of CaixaBank's Governing Bodies.
In particular, the **Regulatory Compliance Function** is responsible for proactively and autonomously ensuring the correct implementation of a *Compliance* management system in the Bank. In order to address this correct implementation, the function is exercised autonomously and independently and the Bank has provided it with the necessary authority and human and technical resources, as established in Section 4 of this Policy.

Regulatory compliance

1.3 Purpose

The purpose of this Policy is to define the Regulatory Compliance Function, the role of which 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 of, or defective 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 legal and regulatory risk and conduct and compliance risk (jointly, "**compliance risks**");as well as advise, inform and assist the senior management and the governance bodies in relation to regulatory compliance, promoting a culture of compliance throughout the organisation by way of training actions, information and raising awareness.

To this end, the Regulatory Compliance Function pursues the following objectives:

- **Supervising compliance risk** arising from the processes and activities carried out by the Bank.
- **Fostering, championing and promoting the corporate values and principles enshrined in the Code of Ethics that** guide the Bank's actions.
- **The promotion of 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.

In addition, the key figures in the function with the highest level of responsibility are:

- Group *Chief Compliance Officer*: ultimately responsible for the Group's Regulatory Compliance Function.
- Country Compliance Manager: ultimately responsible for compliance in each jurisdiction. responsible for monitoring, supervising and coordinating compliance risks at an overall level in each jurisdiction.
- *Chief Compliance Officer:* responsible for the Compliance Function of each entity (CaixaBank, subsidiaries, branches or representative offices, in the case of the USA).
- *AML Manager:* ultimately responsible for compliance in the prevention of money laundering.
- *AML Officer:* fulfils the anti-money laundering compliance responsibilities expressly delegated by the *AML Manager*.

The content of this Policy includes, among other aspects:

- General principles of the Regulatory Compliance Function
- Governance Framework
- Regulatory Compliance Function management framework
- Control Framework
- Reporting Framework

2. Scope of application

This is a corporate-level Policy. Therefore, the principles of action defined apply to CaixaBank and to all its subsidiaries (jointly, the "CaixaBank Group" or the "Group") that engage in any activity exposed to compliance risk. The governance 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 governance bodies, committees and departments, and their principles of action, methodologies, and processes to the contents of this document.

This integration may involve, among other decisions, the approval of their own policy by the subsidiary. This approval will be necessary in those Group companies that need to adapt the contents herein to their own specific situation, whether in terms of the subject matter, the jurisdiction or the relevance of the risk in the subsidiary. Where the risk control and management activities of the subsidiary are carried out directly by CaixaBank, whether due to the materiality of the risk in 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 Group companies shall be informed of the existence of this Corporate Policy and its applicability to such Group companies. The governing bodies of Group companies will abide by this Corporate policy when the operational principles of the Corporate policy are applicable and the subsidiary does not have its own policy, and the content of the corporate Policy lays out principles, obligations and activities that apply directly to the Group company.

In any case, the Regulatory Compliance Function, given its corporate nature, shall ensure that the integration of this Policy in Group companies is proportionate, that any internal policies approved by a Group company are consistent with the corporate policy, and that this is done uniformly throughout the CaixaBank Group.

Lastly, in addition to being a corporate policy, this Policy is also considered the individual policy of CaixaBank, the parent company of the CaixaBank Group.

For the purposes of this Policy, the **Regulatory Compliance Scope** (Appendix I) is made up of the CaixaBank Group companies that meet the following conditions:

- Effective management by CaixaBank, i.e. CaixaBank holds the majority stake or control of the company
- Active company with a long-term outlook[1] in relation to CaixaBank,
- Existence of a company structure, that is to say, that the company has employees
- Development of an activity related to CaixaBank's activity.

In turn, **among the companies within the scope,** a distinction is made between:

- **Subsidiaries that have their own Regulatory Compliance Function:** companies that have their own Regulatory Compliance Function by virtue of their relative critical nature within the Group or given the existence of specific requirements as they are subject to regulations in addition to Spanish and European banking regulations.

[1]The condition of having a long-term outlook will be considered ineffective once two years have elapsed from the decision being made not to include the company in question in the Scope, should it continue to form part of the Group.

- **Subsidiaries without their own Regulatory Compliance Function:** companies that do not have a Regulatory Compliance Unit as they are not subject to regulations in addition to the banking regulations or at which compliance risk is lower on account of the activities undertaken.

The companies included in the **Scope** must supervise and coordinate the implementation of the corporate management and supervision model in the companies that report to them.

Furthermore, at **an international level**, there are two other types of companies within the Scope:

- **International branches:** CaixaBank branches established in countries other than Spain that essentially focus their scope of activity on financing, the provision of guarantees and basic banking services. As a general rule, branches have their own Regulatory Compliance Function based on local legislation requirements.
- **Representative offices:** CaixaBank branches established in countries other than Spain focus on liaising with and supporting Spanish companies operating abroad, as well as foreign companies operating in Spain. As a general rule, they do not have their own Compliance Unit since their compliance risk is reduced due to the activity carried out. Notwithstanding the above, a Compliance Officer will be appointed in those jurisdictions where the regulator so requires.

In addition, the definition of the Group companies included in the different Compliance taxonomies (AML/CTF, Criminal, etc.) is carried out by the specialist teams for each of these risks.

3. Regulatory Framework. Applicable Standards and Regulations

This Policy will be governed by the applicable regulations in force and any regulations that may amend or replace them in the future. In particular, at the date of preparation, among others, the pertinent regulations applicable to the Regulatory Compliance Function are as follows:

- USA - US *Foreign Corrupt Practices Act* (FCPA), 1977.
- Law 35/2003 of 4 November on Collective Investment Schemes.
- Spanish Securities Market Regulator (CNMV) Circular 6/2009, of 9 December, on internal control of collective investment scheme management companies and investment companies.
- Organic Law 5/2010, of 22 June, which modifies Law 10/1995, of 23 November, on the Criminal Code and subsequent modifications (2010).
- UK Bribery Act (2010).
- Royal Decree 1082/2012, of 13 July, approving the Regulations implementing Law 35/2003, of 4 November, on collective investment schemes.
- DIRECTIVE (CRD IV) 2013-36-EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/CE and repealing Directives 2006/48/EC and 2006/49/EC.
- Agreement between the Kingdom of Spain and the United States of America to improve international tax compliance and implementation of the Foreign Account Tax Compliance Act (FATCA), signed in Madrid on 14 May 2013.
- CNMV Circular 1/2014 of 26 February on internal organisation requirements and control functions for investment firms.
- MiFID II Directive 2014/65/EU of 15 May 2014 regarding financial instrument markets and which amends Directive 2002/92/EC and Directive 2011/61/EU.
- Law 10/2014, of 26 June, on the organisation, supervision and creditworthiness of credit institutions. (LOSS).
- Royal Decree 85/2015, of 13 February, implementing Law 10/2014 of 26 June, on the regulation, supervision and solvency of credit institutions.

- Commission Delegated Regulation (EU) 2017/565 of 25 April 2016, supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.
- Directive on the protection of persons who report breaches of EU law (2019).
- Spanish Law 2/2023, of 20 February, on the protection of persons who report regulatory breaches and the fight against corruption.
- Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
- Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.
- Directive (EU) 2024/1654 of the European Parliament and of the Council of 31 May 2024 amending Directive (EU) 2019/1153 as regards access by competent authorities to centralised bank account registries through the interconnection system and technical measures to facilitate the use of transaction records.

The various guidelines and criteria of supervisors, regulators and authorities also apply, such as:

- EBA Guidelines for adequate remuneration policies in virtue of Article 74, Section 3, and Article 75, Section 2, of the Guideline 2013/36/EU and the distribution of information in virtue of Article 450 of the EU Regulation No. 575/2013 (EBA/GL/2015/22).
- Circular 1/2016 of the Spanish Public Prosecution Service on the criminal liability of legal entities, following the reform of the Criminal Code implemented by Organic Law 1/2015 (2016).
- EBA Guidelines of 21 March 2018 on internal governance EBA/GL/2017/11 (2017), adopted by the Bank of Spain on 18 May 2018 and updated on 2 July 2021 (EBA/GL/2021/05), which became effective on 31 December 2021.
- Guidelines on policies and procedures in relation to compliance management and on the role and responsibilities of the person responsible for compliance with AML/CFT in accordance with Article 8 and Chapter VI of Directive (EU) 2015/849 (2022).
- Qualified Intermediary Agreement-Revenue Procedure 2022-43.
- Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2021, (EU) No 1094/2010 and (EU) No 1095/2010.

Lastly, this Policy takes into account other Spanish and international standards in the matter, such as:

- "*Enterprise Risk Management - Integrated Framework*" (COSO I, 1992).
- OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1997).
- OECD Principles of Corporate Governance (1999).
- The UN Convention against Corruption (2003).
- Business principles for countering bribery. International transparency (2003).
- "*Compliance and the Compliance function in Banks*" (Basel Committee on Banking Supervision, 2005).
- "*Enterprise Risk Management - Integrated Framework*" (COSO II, 2004).
- Guidance to the US FCPA (2012) Resource Guide and compilation of information.
- Corporate governance principles for banks (Basel Committee on Banking Supervision, July 2015).

- G20/OECD Principles of Corporate Governance (2016).
- ISO 37001 – Anti-bribery management systems (2016).
- EBA final report "ON THE APPLICATION OF THE GUIDELINES ON THE REMUNERATION OF SALES STAFF". With the aim of ensuring that entities continue to make progress in the area of customer protection, the EBA has identified 17 good practices to be followed by entities in their practical application of the 2016 EBA Guidelines.
- UNE 19601 on Criminal Compliance Management Systems (2017).
- Guide on "COSO *Enterprise Risk Management – Integrating with Strategy and Performance*" (COSO III ERM, 2017).
- CNMC Antitrust *Compliance* Programmes Guidelines (2020).
- ISO 37301 standard for compliance management systems (2021).
- Final guidelines on the MiFID II compliance function - ESMA35-36-1952 (2021).
- Final report issued by ESMA in 2022 on "The Guidelines on Remuneration Policies and Practices" The final report issued by ESMA in 2022 on "The Guidelines on Remuneration Policies and Practices", which includes the responses to the public consultation launched last year and updates the guidelines with the aim of enhancing customer protection against the behaviour of staff of entities that result in possible conflicts of interest or cases of misconduct in the marketing of products and services.
- ESMA Guidelines 35-43-3565 on certain aspects of the MiFID II remuneration requirements.

With regard to Group companies or, where applicable, branches subject to foreign jurisdictions or additional industry regulations, any policies and procedures developed by said Group companies or branches shall take into account, in addition to their own regulations, the obligations at the consolidated level as contained in applicable law and regulations, provided that they do not contradict the specific requirements of the corresponding jurisdiction or industry regulations.

Lastly, the necessary regulations, guidelines or procedures for correct implementation, execution and compliance with this Policy shall be implemented in each of the Group companies or, where applicable, subsidiaries.

4. General principles of the Regulatory Compliance Function

The principles governing the actions of the CaixaBank Group when it comes to the control and management of liquidity risk are:

a) Autonomy

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

b) Independence

To ensure the objectivity of its decisions, the Regulatory Compliance Function shall operate under the principal of functional independence with regard to those areas or functions in relation to which it supervises and monitors compliance risk.

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

Similarly, the appointment, transfer, establishment of its remuneration (both fixed and variable and the proportion between both of them, respecting the principle of reasonableness at all times) and the evaluation of the degree of achievement of its objectives or goals will correspond, subject to compliance with the legal requirements applicable to the corresponding Governance Bodies.

The persons assigned to the Regulatory Compliance Function may not be involved in providing the services or carrying out the activities they oversee, so as to avoid any undue influence in the exercise of their actions.

The Regulatory Compliance Function will in all cases have direct access to the Management and Governance Bodies in the carrying out of its duties and responsibilities.

c) Authority

The Regulatory Compliance Function will at all times be positioned within the Bank's highest hierarchical levels of the Organisation (Senior Management and other key positions, as defined in the Corporate Governance and Internal Control Policy) and will have sufficient authority for its lines of action and decisions to be assumed by other areas of the Bank.

It may, at any time, raise queries, request information, initiate or require evaluation and/or verification processes or investigations relating to the areas or processes that present real or potential risks of non-compliance that may pose a risk to the Bank.

d) Human and technical resources

Due to the importance of the Regulatory Compliance Function and its responsibilities within the organisation, the various areas that perform this function must have sufficient resources to undertake the various activities and responsibilities assigned under the terms of this policy.

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

To this end, it must have a budget that allows it to carry out its activities, in line with the level of risk of non-compliance to which the Bank is exposed.

e) Ability and integrity

All persons assigned the Regulatory Compliance Function must possess the knowledge, experience, qualifications and professional integrity needed to fully and properly carry out these duties throughout the Bank and thereby guarantee an extensive and permanent coverage of the Regulatory Compliance Function.

To this end, training and certification plans must be established to access and carry out the function, as well as plans that nurture its further professional development.

f) Access to information

The Regulatory Compliance Function will have access to as much information and documentation as deemed necessary to adequately carry out its duties; It shall also count on the necessary support across all levels of the organisation so that it is able to report to the supervisory bodies in due course and thus meet its obligations in this regard.

g) Risk-based approach

In the performance of its activity, all the areas involved in compliance with regulations, and in particular the Regulatory Compliance Function, must at all times implement a risk-based approach, and therefore carry out an ongoing evaluation of the compliance risks associated to the main processes, to prioritise the supervisory and monitoring activities that are inherent in it, as well as appropriately allocate the resources according to the risks identified.

h) Permanence

In order to fulfil its legal remit and perform the tasks entrusted to it by law, the Regulatory Compliance Function must exist and form part of the Bank's organisational structure at all times, regardless of the specific individuals that make up the function.

5. Regulatory Compliance Function management framework

5.1 Organisational model

5.1.1. The corporate Regulatory Compliance Function

The corporate Regulatory Compliance Function will report functionally to the Chair of the CaixaBank Risk Committee and hierarchically to the Compliance and Control Department and Public Affairs. This functional dependence means that the CaixaBank Risk Committee participates in the appointment and dismissal of the *Chief Compliance Officer*, whether corporate or Group, as well as in the setting of objectives, the evaluation of their performance and their fixed and variable remuneration.[2].

The Group's *Chief Compliance Officer* is the highest-ranking person responsible for the corporate Regulatory Compliance Function and this position is held by CaixaBank's *Chief Compliance Officer*. The corporate *Chief Compliance Officer* carries out their duties in accordance with the general principles described in Section 4 of this Policy, and in particular, independently and autonomously with regard to the rest of the Bank's bodies. This figure therefore cannot receive instructions of any kind in the exercise of their role and has all the personal and material resources necessary to carry them out.

a) *Appointment*

The Bank's Board of Directors is responsible for appointing the corporate *Chief Compliance Officer*. The appointment must be made:

- In accordance with the European Central Bank's fit and proper assessment guide.
- Taking into account their knowledge, skills and experience, regarded as being suitable for the performance of their duties.

The appointment and dismissal of the *corporate Chief Compliance Officer will be communicated to the relevant authorities.*

b) *Functions*

The corporate *Chief Compliance Officer* will establish a framework for the coordination of relations with the respective Regulatory Compliance units of the companies within the Scope that allows for regular coordination between the Regulatory Compliance Function and these units, as well as reporting flows. In this regard, the framework will determine the appropriate coordination mechanisms based on the competencies of the corporate function described below:

- Establishing general guidelines to ensure proper risk management in relation to compliance and the implementation of a culture of compliance across the Group, in coordination with the responsible areas within Group companies, as well the establishment of any other matters related to the Group it may be entrusted in applicable sectoral regulations (e.g. within the scope of the prevention of money laundering and terrorist financing).

[2] With regard to appointments and dismissals, the Risk Committee advises the Appointments and Sustainability Committee and, in relation to remuneration, it advises the Remuneration Committee.

- Overseeing the definition of the Compliance Plan of the companies within the Scope prior to its approval by their corresponding Governing Bodies, being able to request the inclusion of new activities with the aim that the Plan covers the supervision of all compliance risks.
- Proposal for the creation of collegiate bodies with the Group's scope (e.g. the Group's internal control body within the scope of prevention of the money laundering and of terrorist financing).
- Participation in the processes of appointment, dismissal, setting and validation of goals, performance evaluation and determination of the fixed and variable remuneration of the *Chief Compliance Officers* of the Group companies.
- Ensuring that the personnel involved in Compliance management in the Group companies have the appropriate competences and experience, and that the structure of the function is adequate for the management of compliance risks and is proportionate to the nature, scale and complexity of the activities carried out by each of the Group companies.

5.1.2 CaixaBank's regulatory compliance function

The head of the CaixaBank Regulatory Compliance function is the CaixaBank *Chief Compliance Officer*, who also acts as the Group *Chief Compliance Officer*.

This position is compatible with the appointment of other responsibilities, with the *Chief Compliance Officer* of CaixaBank having been appointed by the Board of Directors as the Head of the Group's Internal Information System, FATCA Responsible Officer, AML Officer and exercising the functions of the AML Manager, among others. The functions derived from each of these appointments are described in the policies that manage each of these risks.

a) *Appointment and remuneration*

The same criteria established in section 5.1.1. regarding the appointment of the Group *Chief Compliance Officer,* are applicable to the CaixaBank *Chief Compliance Officer*.

The remuneration of CaixaBank's *Chief Compliance Officer* and of the personnel in the Regulatory Compliance Function may not be linked to the profit of the areas over which they exercise their oversight responsibilities. Notwithstanding the foregoing, part of the remuneration may consist of variable remuneration subject to the achievement of the Bank's overall targets, which shall always be compatible with adequate and effective risk management.

b) *Functions*

CaixaBank's *Chief Compliance Officer* is responsible for the proper development of the management model of the CaixaBank Regulatory Compliance Function and for carrying out the actions necessary to develop the budget so that the Function fulfils the tasks entrusted to it. Its main responsibilities are as follows:

- Approve and update the document "Regulatory Compliance Regulatory Framework Inventory", which lists the procedures, policies and internal regulations for compliance risks.
- Define, implement and maintain a compliance programme that ensures the proper and efficient implementation of the corporate regulatory compliance policy.
- Identify, monitor and continuously evaluate compliance risks.

- Ensure that the Bank's governance bodies and Senior Management are regularly informed of the most significant aspects of Compliance and of the actions plans put in place to resolve any weaknesses.
- Aid and advise Senior Management and all other Group company and CaixaBank personnel and its subsidiaries on how to properly manage compliance risk.
- Promote, coordinate, monitor and, where applicable, implement the training plans within the scope of Regulatory Compliance for the Bank's employees.
- Maintain ongoing contact with the main regulatory and supervisory bodies in order to understand their expectations and help ensure fluid, two-way communication, which will involve building a strong trust-based relationship and keeping them regularly apprised of CaixaBank's main regulatory initiatives and projects.
- Lead, together with the areas responsible for Corporate Social Responsibility, the process for disseminating the values and principles included in CaixaBank's Code of Ethics.
- Using a risk-based approach, plan the key activities to be carried out by the Regulatory Compliance Function, as well as monitor them. This planning is reflected in the Annual Compliance Plan and is submitted to the Board of Directors for approval.
- Promote a culture of compliance with the regulations within the Organisation, promoting the establishment and maintenance of an adequate governance framework that facilitates the compliance throughout the organisation of the regulations, policies, procedures and standards of conduct.

5.1.3. The Country Compliance function

Similarly, with the aim of ensuring sound management of compliance risk in those jurisdictions where more than one business of the Group or more than one supervised entity operates, the corporate *Chief Compliance Officer* shall appoint as head of the Country Compliance Function (*Country Compliance Manager*), the *Chief Compliance Officer* of the Group company responsible for regulatory compliance in the jurisdiction's main business or entity. Similarly, the *Country Compliance Manager* shall monitor, supervise and coordinate the Group's Compliance risk at an overall level in that jurisdiction.

This function will not entail hierarchical or functional dependencies additional to those defined in this Policy.

5.1.4. The Regulatory Compliance Function in Group companies

Personnel assigned to the Regulatory Compliance Function in Group companies shall act in accordance with the organisational and joint accountability governance model described below:

- **Subsidiaries, branches and representative offices that have their own Regulatory Compliance Function**: The person responsible for the function or *Compliance Officer* of each of these entities will have a dual reporting relationship: hierarchically, to the CEO, Managing Director or equivalent, or to the governance body directly; and, on the other hand, functionally, to the corporate *Chief Compliance Officer*. Decisions affecting the officer's appointment, removal and remuneration (both fixed and variable and the proportion between both, respecting the principle of reasonableness at all times) and the task of evaluating the attainment of his or her objectives or targets will correspond, subject to compliance with applicable legal requirements, to his or her direct hierarchical superior, together with the *Chief Compliance Officer*. The Governance Body will be informed of any decision that affects these actions.

The duties attributed to the *Compliance Officers* of the Group companies and their remuneration and appointment will be determined based on the provisions of this Policy in Section 5.1.2 for CaixaBank's *Chief Compliance Officer*, as well as, where appropriate, the functions resulting from the appointment of other positions such as the AML Manager.

Regulatory compliance

- **Subsidiaries and representative offices that do not have dedicated staff assigned to the Regulatory Compliance Function:** The function will be carried out by the CaixaBank Compliance function. The subsidiary company, branch, or representative office shall appoint someone from Senior Management to act as liaison between them and CaixaBank.

5.2 Management model

The management model of the Regulatory Compliance Function has two main pillars:

a) Taxonomy of compliance risks
b) Remit of the Regulatory Compliance Function within the control environment: Three lines of defence model

5.2.1 Taxonomy of compliance risks

The compliance risk taxonomy is a classification by categories of the conduct and compliance risks and legal and regulatory risks to which the Group is exposed, based on the corporate catalogue of risks of the CaixaBank Group.

The classification of compliance risk into different categories ensures a clearer understanding of the various actions to be undertaken by the Regulatory Compliance Function and creates a starting point, or baseline, for the ongoing assessment of these risks.

It also provides the basis for identifying and prioritising the activities on which the Regulatory Compliance Function should focus during the year (Annual Compliance Plan), for updating of the list of compliance weaknesses and deficiencies and for undertaking initiatives and projects within the Regulatory Compliance Department.

In accordance with CaixaBank's corporate internal control policy, the Regulatory Compliance Function is responsible for supervising the following risks, from among those set out in the corporate risks catalogue:

- Conduct and compliance.
- Legal and Regulatory.

The risks to be supervised may vary due to legal requirements or express supervisory criteria, as provided for in Section 2 of this Policy. The sub-categories that make up this compliance risk taxonomy undergo annual reviews by the Global Risks Committee.

5.2.2. Remit of the Regulatory Compliance Function within the control environment: Three lines of defence model

As part of the Group's internal control framework and in line with the guidelines set out in the corporate internal governance and internal control policies, the Regulatory Compliance Function oversees and manages the conduct and compliance risk and the legal and regulatory risk already identified in the taxonomy of corporate risks, following the three lines of defence structure, in which the duties and responsibilities of each line of defence are clearly defined.

The Regulatory Compliance Function, as the internal control function forming the second line of defence and in accordance with the corporate governance and internal control policy, identifies, measures, defines and monitors conduct and compliance risk appetite and legal and regulatory risk, and is also tasked with independently reviewing the effective application of policies and procedures by the first line of defence. The Regulatory Compliance Function acts independently from the business units, ensuring the existence of policies for the management and control of the compliance risks, monitoring its application, evaluating the control environment and reporting all material risks.

5.3 Key elements of the Regulatory Compliance Function

The Regulatory Compliance Function makes use of the following key elements to ensure adequate coverage for compliance risks:

- Compliance programme
- Annual compliance plan
- Weakness identification process

5.3.1 Compliance programme

The compliance programme is essentially a collection of processes and activities there to streamline and systematise the main activities and functions of the Compliance function, following a generally accepted methodology at international level.

The compliance programme is applied through a series of key activities, including:

5.3.1.1 Regulatory compliance policies

A crucial element of the CaixaBank compliance programme is the existence and regular updating of regulatory compliance policies that clearly set out the requirements and criteria that the Bank must follow with regard to compliance risk.

5.3.1.2. Implementation and monitoring of legislative and regulatory changes

It consists either of the implementation of regulations that have an impact on the area of compliance risks, or of monitoring them when their implementation corresponds to other affected areas.

5.3.1.3 Risk map and indicators

This requires the creation and maintenance of an inventory of key regulations that affect CaixaBank's activities and that are related to the taxonomy of compliance risks, as well as the identification, implementation and monitoring of indicators to monitor, detect and mitigate such risks.

5.3.1.4 Advisory services

As previously described, the Regulatory Compliance Function is entrusted with the crucial task of providing advice to the Governance Body and Senior Management and the rest of the organisation on all relevant aspects related to the purpose of Regulatory Compliance. When carrying out this role, the Compliance Function must be able to rely on the support of other specialised departments within the Bank, if this support is needed, depending on the matter at hand.

5.3.1.5 Regular assessment of compliance risks

Regular risk assessments are a key feature of the Bank's compliance programme and are used to prioritise the activities to be carried out by the Compliance function and to establish their criticality and allocate resources accordingly.

The compliance risk assessment must address the risk inherent in the Bank's activities, together with the results of the control environment monitoring process, the relevant findings of the internal and external auditors and supervisory bodies, and the work carried out by Customer Service Department, as well as any queries or complaints submitted via the relevant channels, which the Compliance function is responsible for handling.

5.3.1.6 Monitoring and testing

The Regulatory Compliance Function employs monitoring and testing techniques to evaluate the compliance risk control environment, with a risk-based approach.

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 action deriving from non-compliance with applicable law and regulations.

The tests involve validating compliance with law and regulations related to compliance risk in the Bank's day-to-day processes, by way of independent verification techniques such as samplings, process reviews, or any other type of testing.

5.3.1.7 Training and awareness raising

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

5.3.1.8 Communication and reporting

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

It will regularly report to the Governing Bodies.

5.3.2 Annual compliance plan

The Annual Compliance Plan, approved by the Board of Directors, contains a list of activities of the Regulatory Compliance Function during said period (one calendar year), together with a schedule for its execution, and all with the aim of guaranteeing that the activities that are exposed to risk are regularly reviewed, evaluated and communicated.

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

The Annual Compliance Plan will be regularly monitored so as to ensure that the management and governance bodies are kept abreast of the main conclusions and findings regarding the plan, the degree of achievement with respect to the initial planning and the most significant changes that have arisen.

5.3.3 Deficiency identification process

The process of identifying deficiencies is the key element that the Regulatory Compliance Function has in order to comply with the second line of defence mandate of the compliance risks and to report to Senior Management.

Compliance deficiencies are any identified weakness in the control environment associated with compliance risks, resulting in:

- Non-compliance with prevailing law or regulations in relation to the risks managed by the Compliance function.
- Business practices carried out by the Bank and/or among its employees that are inappropriate or contrary to the *Code of Ethics and implementing rules and regulations*.

The detected deficiencies may arise when implementing any of the key activities that make up the Compliance Programme and which are normally reflected in the Annual Compliance Plan, or that come to light during inspections by supervisory bodies and the internal and external auditors, revealing deficiencies or weaknesses in the control environment.

VidaCaixa Annexe to the *Corporate Regulatory Compliance Policy*

VidaCaixa Regulatory Compliance

May - 2025

Regulatory framework applicable to VidaCaixa's regulatory compliance function.

This Annex sets out the regulations of the insurance sector that are specifically applicable to Vidacaixa's compliance function in addition to the CaixaBank Group Corporate Regulatory Compliance Policy:

- Spanish Law 20/2015, of 14 July, on the Regulation, Supervision and Solvency of Insurance and Reinsurance Companies (LOSSEAR)
- Spanish Royal Decree 1060/2015, of 20 November, on the regulation, supervision and solvency of insurance and reinsurance companies (ROSSEAR)
- "*Guidelines on System of Governance*" EIOPA-BoS-14/253 EN, of the European Insurance and Occupational Pensions Authority (EIOPA).