



General Principles of the Corporate Regulatory Compliance Policy

20 February 2025

Contents

1. Introduction	3
1.1 <i>Background</i>	3
1.2 <i>Scope</i>	3
1.3 <i>Purpose</i>	3
2. Scope of application	5
3. Regulatory framework. Applicable standards and regulations	6
4. General principles of the Regulatory Compliance Function	9
5. Regulatory Compliance Function management framework	11
5.1 Organisational model	11
5.1.1 <i>The Corporate Regulatory Compliance Function</i>	11
5.1.2 <i>CaixaBank's Regulatory Compliance Function</i>	12
5.1.3 <i>The Country Compliance Function</i>	13
5.1.4 <i>The Regulatory Compliance Function in Group companies</i>	13
5.2 Management model	14
5.2.1 <i>Compliance risk taxonomy</i>	14
5.2.2 <i>Remit of the Regulatory Compliance Function in the control environment: three lines of defence model</i>	15
5.3 Key components of the Regulatory Compliance Function	15
5.3.1 <i>Compliance programme</i>	15
5.3.1.1 <i>Regulatory compliance policies</i>	15
5.3.1.2 <i>Implementation and monitoring of legislative and regulatory changes</i>	15
5.3.1.3 <i>Risk map and indicators</i>	16
5.3.1.4 <i>Advisory services</i>	16
5.3.1.5 <i>Regular assessment of compliance risks</i>	16
5.3.1.6 <i>Monitoring and testing</i>	16
5.3.1.7 <i>Training and awareness-raising</i>	16
5.3.1.8 <i>Communication and reporting</i>	17
5.3.2 <i>Annual Compliance Plan</i>	17
5.3.3 <i>Shortcomings identification process</i>	17

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" interchangeably) promoting ethical business principles, reaffirming a corporate culture of respect for the law and regularly verifying and assessing the effectiveness of controls related 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 this scenario, it is essential to have a Compliance Function within the Bank and to ensure that it has an organisational and management model which complies with applicable regulations and the highest national and international standards.

Compliance is the responsibility of each and every member of the organisation, i.e. all employees, officers, directors 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. 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 whose role is to identify, evaluate, oversee and report on the risks of sanctions or financial losses to which the Bank is exposed as a result of its failure to comply or improper/inadequate compliance with laws, regulations, legal or administrative requirements, codes of conduct, ethical standards and good practices relating to its area of activity with reference to legal and regulatory risks and conduct and compliance risks (jointly, "**compliance risks**"); as well as to advise, inform and assist senior management and governing bodies in regulatory compliance by promoting a culture of compliance across the organisation through training, information and awareness-raising activities.

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 the principles enshrined in the Code of Ethics** that guide the Bank's actions.
- **Promoting a culture of control and compliance with the laws and regulations in force** (both external and internal) that enables and fosters their integration into the management of the entire 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. They are tasked with 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 representation offices in the case of the USA).
- AML Manager: ultimately responsible for anti-money laundering compliance.
- 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 governing bodies of these companies will make the appropriate decisions in order to integrate the provisions of this Policy. In keeping with the principle of proportionality, the governance framework will be adapted to the characteristics of their structure of governing bodies, committees and departments, and their principles of action, methodologies and processes will be adapted to the contents of this document.

This integration may prompt the subsidiary to approve its own policy. Approval is required in those Group companies that need to adapt the provisions of this Policy to their own circumstances, whether in terms of matter, jurisdiction or the relevance of the risk in the subsidiary. Where the subsidiary's risk control and management activities 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 Group companies concerned will be made aware 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, the subsidiary does not have its own policy and the content of the Corporate Policy lays out principles, obligations and activities that have to be performed directly by the Group company.

In any case, the Regulatory Compliance Function, given its corporate role, will ensure that the integration of this Policy in Group companies is proportionate, any internal policies approved by a Group company are aligned with corporate policy, and that there is consistency throughout the CaixaBank Group.

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

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

- Effective management by CaixaBank, that is, CaixaBank holds the majority stake or control of the company
- Active company with a long-term commitment¹ by CaixaBank
- Existence of a company structure, that is, that the company has employees
- Performance of an activity related to CaixaBank's activity.

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

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

¹The condition of having a long-term commitment will cease to apply if two years after the decision not to include it in the Scope, the company continues to be part of the Group.

- **Subsidiaries without their own Regulatory Compliance Function:** companies that do not have their own Regulatory Compliance Unit because they are not subject to regulations other than banking regulations or where the compliance risk is lower due to the activity undertaken.

The companies included in the **Scope** must supervise and coordinate the implementation of the corporate management and supervision model in the companies reporting 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 focus their activities primarily on financing, the provision of guarantees and core banking services. As a general rule, branches have their own Regulatory Compliance Function based on local legislation requirements.
- **Representation offices:** CaixaBank branches established in countries other than Spain that focus their activity 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 less due to the activity carried out. Notwithstanding the foregoing, a Compliance Officer will be appointed in those jurisdictions where the regulator so requires.

In addition, the Group companies included in the different compliance taxonomies (AML/CTF, Criminal, etc.) are specified 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 that may amend or replace them in the future. In particular, at the date of preparation the regulations applicable to the Regulatory Compliance Function are as follows:

- US Foreign Corrupt Practices Act (FCPA), 1977
- Act 35/2003 of 4 November on collective investment undertakings
- Spanish National Securities Market Commission (CNMV) Circular 6/2009 of 9 December on internal control of collective investment undertaking management companies and investment companies.
- Act 5/2010 of 22 June amending Act 10/1995 of 23 November on the Criminal Code and its subsequent amendments (2010)
- UK Bribery Act (2010)
- Royal Decree 1082/2012 of 13 July enacting the implementation regulations of Act 35/2003 of 4 November on collective investment undertakings
- Directive (CRD IV) 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC 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
- Directive (MiFID II) 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU

- Act 10/2014 of 26 June on the organisation, supervision and solvency of credit institutions (LOSS).
- Royal Decree 85/2015 of 13 February implementing Act 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 (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law
- Act 2/2023 of 20 February regulating the protection of people who report on regulatory violations and anti-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 supervisory bodies, regulators and authorities also apply, including:

- EBA Guidelines on sound remuneration policies pursuant to Articles 74(3) and 75(2) of Directive 2013/36/EU and disclosure of information pursuant to Article 450 of Regulation (EU) No 575/2013 (EBA/GL/2015/22)
- Circular 1/2016 of the State Attorney General's Office on the criminal liability of legal entities following the reform of the Criminal Code implemented by Act 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 pursuant to 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 1093/2010, (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. Transparency International (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 standard on 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 entities continue to make progress in 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 standard 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 on compliance management systems (2021)
- Final Guidelines on the MiFID II Compliance Function - ESMA35-36-1952 (2021)
- 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 results 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

In the case of Group companies or, where applicable, branches subject to foreign jurisdictions or additional industry regulations, any policies and procedures drawn up by these Group companies or branches will take into account, in addition to their own regulations, the obligations at the consolidated level contained in the regulations referenced above as long as they do not contradict the specific requirements of the corresponding jurisdiction or industry regulations.

Lastly, each Group company or, where applicable, each branch will draw up the regulations, guidelines or procedures required for the proper implementation and performance of and compliance with this Policy.

4. General principles of the Regulatory Compliance Function

The principles governing the CaixaBank Group's actions to control and manage compliance risks are:

a) Autonomy

Regulatory Compliance is an autonomous function, which means that it will have sufficient initiative to carry out its duties without needing to receive specific instructions from other areas or act on their behalf.

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

b) Independence

To ensure the objectivity of its decisions, the Regulatory Compliance Function will operate under the principle of functional independence from those areas or functions where it oversees and monitors compliance risks.

Likewise, in order to guarantee its independence, the Regulatory Compliance Function will not be subject to the fulfilment of commercial objectives and only to those relating to its own activity and the Bank's overall corporate challenges.

Likewise, appointment, removal, determination of remuneration (both fixed and variable and the proportion between them, always respecting the principle of reasonableness) and evaluation of how far its objectives or challenges have been achieved will be the responsibility of the relevant governing bodies subject to compliance with applicable legal requirements.

Staff assigned to the Regulatory Compliance Function may not take part in the provision of services or conducting activities under their supervision to avoid any undue influence in the performance of their duties.

The Regulatory Compliance Function will always have direct access to Management and Governing Bodies in the performance of its duties and responsibilities.

c) Authority

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

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

d) Human and technical resources

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

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

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

e) **Ability and integrity**

All individuals performing the Regulatory Compliance Function must have the knowledge, experience, qualifications and professional integrity needed to fully and properly carry out their duties in the Bank, thus ensuring broad coverage of the Regulatory Compliance Function on an ongoing basis.

To this end, training and certification programmes must be established for access to and performance of the role together with staff professional development plans.

f) **Accessing information**

Regulatory compliance will have access to all information and documentation necessary to properly carry out its duties; it will also have the necessary support at all levels to enable it to meet the information requirements of supervisory bodies within the specified deadlines.

g) **Risk-based approach**

In the performance of their duties, all areas involved in regulatory compliance, and in particular the Regulatory Compliance Function, must always implement a risk-based approach and therefore continuously assess the compliance risks associated with core processes to prioritise their specific supervision and monitoring activities and allocate resources appropriately based on the identified risks.

h) **Permanence**

In order to fulfil the mission and tasks assigned to it by current regulations, there must be a Regulatory Compliance Function in the Bank's organisational structure at all times, regardless of the specific individuals who are part of it.

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 and Public Affairs Department. This functional reporting means that the CaixaBank Risk Committee takes part in the appointment and removal of the Chief Compliance Officer whether corporate or Group, setting targets and assessing 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 performs their duties under the general principles described in section 4 of this Policy, and in particular independently and autonomously from the rest of the Bank's bodies. They thus cannot be given instructions of any kind in their role and will have all the staff and material resources required to carry it 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, considering them suitable for the performance of their duties.

The appointment and removal of the corporate Chief Compliance Officer will be reported to the relevant authorities.

b) *Functions*

The corporate Chief Compliance Officer will establish a framework for coordinating relationships 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 management of compliance risks and implementing a compliance culture across the Group in coordination with the responsible areas in the Group's companies together with establishing any others relating to the Group that may be entrusted to it in applicable industry regulations (for example, in anti-money laundering and counter-terrorism financing).

² The Risk Committee advises the Appointments and Sustainability Committee on appointment and removal and the Remuneration Committee on remuneration.

- Overseeing the definition of the Compliance Plan for companies within the Scope prior to its approval by their corresponding Governing Bodies and requesting the inclusion of new activities to ensure that the Plan covers oversight of all compliance risks.
- Proposing in certain areas the creation of collegiate bodies with Group scope (for example, the Group's internal control body in anti-money laundering and counter-terrorism financing).
- Taking part in the processes of appointment, removal, setting and validating challenges, performance assessment and deciding on fixed and variable remuneration for the Chief Compliance Officers of the Group's companies.
- Ensuring that staff involved in managing regulatory compliance in the Group's companies have the appropriate skills and experience and that the structure of the function is appropriate for managing compliance risks and proportionate to the nature, scale and complexity of the activities carried out by each of the Group's companies.

5.1.2 CaixaBank's Regulatory Compliance Function

The head of CaixaBank's Regulatory Compliance Function is CaixaBank's Chief Compliance Officer, who also acts as the Group's Chief Compliance Officer.

This position is compatible with appointment to other responsibilities, and so CaixaBank's Chief Compliance Officer has been appointed by the Board of Directors as Head of the Group's Internal Information System, FATCA Responsible Officer and AML Officer exercising the duties of this post and those delegated by the AML Manager. 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's Chief Compliance Officer are applicable to CaixaBank's Chief Compliance Officer.

The remuneration of CaixaBank's Chief Compliance Officer and staff 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 compensation tied to the achievement of the Bank's overall targets which will always be compatible with appropriate 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 taking the steps needed to implement the budget to enable the Compliance Function to carry out its assigned tasks. Their main responsibilities are:

- Approving and updating the "Regulatory Compliance Regulatory Framework Inventory" document which lists the procedures, policies and internal regulations for compliance risks.
- Defining, implementing and maintaining a compliance programme that ensures proper and effective implementation of the corporate regulatory compliance policy.
- Identifying, monitoring and continuously evaluating compliance risks.

- Ensuring that the Bank's Governing Bodies and Senior Management are regularly informed of the most significant aspects of regulatory compliance and the actions plans put in place to address any weaknesses.
- Assisting and advising Senior Management and other staff at CaixaBank and the Group's companies on how to properly manage compliance risk.
- Promoting, coordinating, monitoring and, where appropriate, implementing training plans for the Bank's employees in regulatory compliance.
- Maintaining ongoing contact with key regulatory and supervisory bodies to understand their expectations and help ensure seamless communication, including developing a relationship based on mutual cooperation and keeping them regularly apprised of CaixaBank's main regulatory initiatives and projects.
- Leading, together with the areas in charge of Corporate Social Responsibility, the process of publicising the values and principles included in CaixaBank's Code of Ethics.
- Planning using a risk-based approach the key activities to be carried out by the Regulatory Compliance Function during the year and monitoring them. This planning is reflected in the Annual Compliance Plan and submitted to the Board of Directors for approval.
- Promoting a culture of regulatory compliance within the Organisation by driving the establishment and maintenance of an appropriate governance framework which enables compliance with regulations, policies, procedures and standards of conduct across the organisation.

5.1.3. The Country Compliance Function

To ensure sound management of compliance risks in jurisdictions where more than one Group business or more than one supervised entity operates, the corporate Chief Compliance Officer will appoint as Country Compliance Manager the Chief Compliance Officer of the Group company responsible for regulatory compliance in the jurisdiction's main business or entity. The Country Compliance Manager will monitor, supervise and coordinate compliance risks at an overall level in that jurisdiction.

This function will not entail any additional hierarchical or functional reporting other than as defined in this Policy.

5.1.4. The Regulatory Compliance Function in Group companies

Staff 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 representation 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 twofold reporting relationship: hierarchically, to the CEO, Managing Director or equivalent, or directly to the governing body; and functionally, to the corporate Chief Compliance Officer. Decisions affecting their appointment and removal and setting remuneration (both fixed and variable and the proportion between them, respecting the principle of reasonableness at all times) and evaluating how far their targets or challenges have been achieved will be made by their direct hierarchical superior together with the Chief Compliance Officer subject to conformity with applicable legal requirements. The Governing Body will be informed of any decisions affecting these actions.

The duties assigned to the Compliance Officers of 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 along with any duties resulting from appointment to other positions such as AML Manager.

Regulatory compliance

- **Subsidiaries and representation offices that do not have dedicated staff assigned to the Regulatory Compliance Function:** the function will be carried out by CaixaBank's Compliance Function. The subsidiary, branch or representation office will appoint a senior management officer to liaise with CaixaBank.

5.2 Management model

The Regulatory Compliance Function management model has two main pillars:

- a) Compliance risk taxonomy
- b) Remit of the Regulatory Compliance Function in the control environment: three lines of defence model

5.2.1 Compliance risk taxonomy

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 CaixaBank Group's corporate risk catalogue.

Dividing compliance risks into different categories makes it easier to define the scope of the Regulatory Compliance Function's actions and provides the starting point for conducting an ongoing assessment of these risks.

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

In accordance with CaixaBank's Governance and Internal Control Policy, the Regulatory Compliance Function is responsible for overseeing the following risks included in the Corporate Risk Catalogue:

- Conduct and compliance.
- Legal and regulatory.

The risks to be supervised may vary due to legal requirements or express supervisory discretion as provided for in Section 2 of this Policy. The subcategories making up this compliance risk taxonomy are reviewed every year by the Global Risk Committee.

5.2.2. Remit of the Regulatory Compliance Function in 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 Governance and Internal Control Policy, the Regulatory Compliance Function oversees and manages conduct and compliance risk and legal and regulatory risk already identified in the corporate risk taxonomy 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 risk appetite for conduct and compliance and legal and regulatory risk. It is tasked with independently reviewing the application of policies and procedures by the first line of defence. The Compliance Function operates independently of the business units, ensuring the existence of management and control policies for compliance risks, monitoring their application, assessing the control environment and reporting all material risks.

5.3 Key components of the Regulatory Compliance Function

The Regulatory Compliance Function uses the following key components to ensure appropriate coverage for compliance risks:

- Compliance programme
- Annual compliance plan
- Weakness identification process

5.3.1 Compliance programme

The compliance programme is the processes and activities that streamline and systematise the main activities of the Compliance Function following an internationally accepted methodology.

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

5.3.1.1 Regulatory compliance policies

A crucial part of CaixaBank's compliance programme is establishing and updating regulatory compliance policies that clearly set out the requirements and criteria the Bank has to follow in relation to compliance risks.

5.3.1.2. Implementation and monitoring of legislative and regulatory changes

This consists of either the implementation of regulations that impact compliance risks or monitoring them when their implementation concerns other affected areas.

5.3.1.3 Risk map and indicators

This involves putting together and keeping an inventory of key regulations that affect CaixaBank's business related to the compliance risk taxonomy coupled with identifying, implementing and tracking indicators to monitor, detect and mitigate these risks.

5.3.1.4 Advisory services

As described above, the Compliance Function is tasked with advising the Governing Body, Senior Management and the rest of the organisation on all relevant aspects related to the Regulatory Compliance mission. When carrying out this role, the Compliance Function must be able to rely on the support of other specialised departments within the Bank, where this support is needed, depending on the matter at hand.

5.3.1.5 Regular assessment of compliance risks

Regular compliance 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 along with establishing their criticality and allocating resources accordingly.

Compliance risk assessment must address the risk inherent in the activity together with the results of the control environment oversight process, the relevant conclusions of internal or external audits and supervisory bodies and the work of the Customer Service Department or the queries or messages submitted via the channels set up for this purpose and which the Compliance Function handles.

5.3.1.6 Monitoring and testing

The Regulatory Compliance Function uses monitoring and testing techniques to assess the compliance risk control environment under a risk-based approach.

Monitoring involves regular tracking and review of activities based on key risk indicators (KRIs) or internal decisions for early detection of deviations or inappropriate actions resulting from failure to comply with regulations.

Testing involves validating compliance with regulations related to compliance risks in the Bank's routine processes using independent verification techniques such as sampling, process reviews or any other type of testing.

5.3.1.7 Training and awareness-raising

To fulfil its mission, the Regulatory Compliance Function runs ongoing training, communication and awareness programmes for all staff to promote a culture of compliance and understanding of compliance obligations and responsibilities. These training activities will be set out in the Annual Training Plan in close partnership with Human Resources.

5.3.1.8 Communication and reporting

The Compliance Function fosters an appropriate governance framework for promptly and effectively escalating and reporting any significant control weaknesses related to compliance risks to the bank's governing 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 the activities of the Regulatory Compliance Function during the period to which it refers (one calendar year) along with a schedule for its performance to ensure that activities exposed to risk are regularly reviewed, assessed and reported.

The principles of proportionality and a risk-based approach are used to define and prioritise these activities. Based on the results of the risk assessment, the risks identified previously and the forecast supervisory actions, the key activities to be implemented throughout the year are designed and planned.

The Annual Compliance Plan will be regularly reviewed for the purpose of briefing Management and Governing Bodies on the Plan's main conclusions, how much of it has been completed compared to the original plan, and any major changes that may have come up.

5.3.3 Shortcomings identification process

The process of identifying shortcomings is the key tool available to the Regulatory Compliance Function to fulfil its mandate as the second line of defence against compliance risks and report to Senior Management.

Compliance shortcomings are any weaknesses identified in the control environment associated with compliance risks resulting in:

- Non-compliance with current legislation or 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 implementing regulations

The shortcomings identified may emerge when implementing any of the key activities making up the Compliance Programme and which are normally reflected in the Annual Compliance Plan, or come to light during checks and inspections by supervisory bodies and internal and external auditors revealing shortcomings in the control environment.