



# General Risk Control and Management Foundations of the Iberdrola Group

25 March 2025

1. Scope of Application	2
2. Purpose	2
3. Risk Management Mechanisms	3
4. Category of Risks	3
5. Comprehensive Risk Control and Management System	4
6. Supervision of the Comprehensive Risk Control and Management System	5
7. Implementation and Monitoring	6



The Board of Directors of IBERDROLA, S.A. (the “**Company**”) has the power to design, assess and continuously revise the Company’s Governance and Sustainability System, and specifically to approve and update the foundations or policies, which contain the guidelines governing the conduct of the Company, and furthermore, to the extent applicable, inform the policies that the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the “**Group**”), decide to approve in the exercise of their autonomy. In exercising these powers and within the framework of applicable legal provisions, the By-Laws and the Purpose and Values of the Iberdrola Group, the Board of Directors hereby approves these General Risk Control and Management Foundations of the Iberdrola Group (the “**Foundations**”) which respects, further develops and adapts the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group with respect to the Company.

## 1. Scope of Application

These Foundations apply to all of the Companies of the Group, as well as to the companies in which the Company holds an equity interest that do not form part of the Group but over which it has effective control, within the limits established by legal provisions and by their respective governance and sustainability systems.

Without prejudice to the provisions of the preceding paragraph, to the extent that listed country subholding companies form part of the Group, they and their subsidiaries, under their own special framework of enhanced autonomy, may establish principles and rules, which must have content consistent with the provisions of these Foundations.

## 2. Purpose

The purpose of these Foundations is to establish mechanisms for the management of risks, identify the main risks faced by the companies of the Group given the nature of its activities and the markets in which it operates, and establish the general framework of action for the configuration of the Comprehensive Risk Control and Management System and for the regular monitoring thereof and the supervision of the internal risk control and management systems.

These Foundations are further developed and supplemented by guidelines and limits that may be established in relation to certain corporate or business risks and which are also subject to approval and review by the Company’s Board of Directors (the “**Guidelines**”), upon a proposal of the Audit and Risk Supervision Committee.

Furthermore, these Foundations and the Guidelines are supplemented with the policies and rules making up the Company’s Governance and Sustainability System or the governance and sustainability systems that the other companies of the Group approve in the exercise of their powers and of their autonomy.

It is the responsibility of the country subholding companies to adopt the Foundations, as well as the Guidelines approved by the Company’s Board of Directors and to specify the application thereof, approving any specific guidelines and risk limits, taking into account the needs, characteristics and particularities of the businesses and of the various countries or territories.

The management decision-making bodies of the head of business or country companies (the “**Head of Business or Country Companies**”) must approve the specific risk limits applicable to each of the guidelines and risk limits approved by the country subholding companies and implement the control systems necessary to ensure compliance therewith, for which purpose they will take into consideration the risk guidelines and limits established by the corresponding country subholding company.



### 3. Risk Management Mechanisms

The Group's companies are affected by various risks inherent to the nature of their activities and to the different countries, territories, businesses, industries and markets in which they operate, which may hinder or prevent the achievement of their objectives and the successful implementation of their strategies.

Aware of the significance of this issue, the Board of Directors of the Company undertakes to develop measures so that, in the exercise and within the limits of its powers, the significant risks to the activities and businesses of the Group's companies are adequately identified, measured, managed and controlled. In particular, it establishes mechanisms for the appropriate management of the risk/opportunity ratio with a level of risk that allows it to:

- a. Attain Group-level strategic objectives with controlled volatility.
- b. Provide the maximum level of assurance to the shareholders.
- c. Protect the interests of shareholders and the financial community, customers and other Stakeholders of the Group's companies.
- d. Protect Group-level results and reputation.
- e. Ensure corporate stability and financial strength in a sustained fashion over time.
- f. Raise awareness of the risk culture among the professionals of the Group's companies through communication and training programmes.

In this regard, all actions aimed at controlling and mitigating risks shall conform to: (i) the main principles of conduct in relation to risk management set out in the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group; (ii) the particularities that may be established for each matter in the policies and regulations of the Company's Governance and Sustainability System or of the governance and sustainability systems approved by the other companies of the Group in the exercise of their powers and autonomy; and (iii) the provisions of the Guidelines that may establish the basic rules of conduct, among other aspects.

### 4. Category of Risks

From a general viewpoint, a risk is considered to be any threat that an event, action or omission may prevent the Group's companies from reaching their objectives and successfully carrying out their strategies.

The classification of risks to which the Group's companies are subject given the nature of their activities and the markets in which they do business are generally those listed below:

- a. **Governance and sustainability risks:** risks arising from a potential breach of the provisions of the governance and sustainability systems, including anti-corruption and anti-fraud legal provisions, of each company of the Group.
- b. **Business and market risks:** risks related to key variables intrinsic to the various activities of the Company and of the other companies of the Group through their businesses, such as the characteristics of demand, product portfolio positioning and management, as well as the uncertainty generated by the volatility of market prices for fundamental variables including electricity, gas or raw material prices.
- c. **Credit and financial risks:** risks related to the possibility that a counterparty breaches its contractual obligations, thus causing an economic or financial loss to the Company or the other companies of the Group, including the risks of payment and costs of replacement, as well as risks related to the volatility of variables (such as exchange rate, interest rate or inflation) and those related to solvency and liquidity.



- d. **Strategic, regulatory, tax and level risks:** risks associated with the macroeconomic, geopolitical and social environment, as well as those arising from regulatory changes or changes to tax regulations. They also include risks associated with the strategy of the Company and the other companies of the Group, such as investment and divestment decisions, or those motivated by the competitive environment.
- e. **Operational risks:** risks referring to direct or indirect economic losses resulting from external events, errors or inadequate internal procedures, as well as those affecting the ability to properly respond to events of any kind that affect the continuity of core processes.
- f. **Technological and comprehensive security risks:** risks related to the appropriate management and operation of information technologies (“IT”) and operational technologies (“OT”), as well as those resulting from the adoption of new technologies, including artificial intelligence. They also include risks related to the security of individuals, tangible and intangible assets and information systems, including cybersecurity, as well as the privacy of the personal data that are processed and compliance with related regulations.

For these risks, their potential negative impact on the value of the Group’s companies resulting from conduct on the part of the corresponding company that is below the expectations created among the various Stakeholders, as defined in the Stakeholder Engagement Policy, and which could generate a reputational risk, will be taken into account.

Given the multidimensional nature of the risks, the taxonomy contemplates additional classification variables to improve the monitoring, control and reporting thereof, including, among others, emerging risks, understood as possible new threats with an uncertain impact and undefined probability, that are growing and that could eventually become material for the Group’s companies.

## 5. Comprehensive Risk Control and Management System

These Foundations are implemented through the design of a Comprehensive Risk Control and Management System, understood as the global operational model for the identification, assessment, control and management of the material risks faced by the Company and the other companies of the Group.

This Comprehensive Risk Control and Management System is based on the provisions of the Ethical and Basic Principles of Governance and Sustainability of the Iberdrola Group, as well as the basic guidelines that might be established along with the risk appetite, mainly in the Guidelines, established within the framework of these Foundations, as well as in the objectives and strategic plan established at the Group level, with the range of mechanisms, material activities and control frameworks developed for such purpose combined under a common methodology and taxonomy.

The Comprehensive Risk Control and Management System is designed in accordance with best international practices in the control and management of business risks, and it includes the following elements:

- a. The ongoing identification of significant risks and threats (including contingent liabilities and other off-balance sheet risks), taking into account their possible impact on strategy, key management objectives, the accounts and the reputation of the Group’s companies.
- b. The analysis and assessment of such risks, both at each of the businesses or corporate areas and taking into account their combined effect on the Group’s companies as a whole, for which purpose the use of common risk measurement, control and quantification standards will be promoted.



- c. The development of due diligence, control and monitoring systems for compliance with policies, including prevention, detection and mitigation mechanisms for the potential situations involving risks that might arise.
- d. The establishment of a structure of guidelines and risk limits and indicators, as well as of the corresponding mechanisms for the approval and implementation thereof, which review and dictate the risk appetite with respect to certain specific risks of the Group's companies, which are approved by the Company's Board of Directors and, if applicable, by the other companies of the Group in accordance with the provisions of these Foundations, and reviewed on at least an annual basis.
- e. The ongoing evaluation of the suitability and efficiency of applying the system and the best practices and recommendations in the area of risks for potential inclusion thereof in the model.
- f. The implementation of internal reporting and control systems to control and manage risks.
- g. Audit of the Comprehensive Risk Control and Management System.

An appropriate allocation of duties and responsibilities at the operational and supervisory level has been established at the Group level for the various significant risks and threats, as well as procedures, methodologies and tools to support the Comprehensive Risk Control and Management System, in which the various corporate and business areas and functions participate. The following participate in this regard:

- (i) The corporate and business areas, which are ultimately responsible for identifying, managing and controlling the risks affecting the matters within their purview ("**risk owners**").
- (ii) Those responsible for the definition, implementation, rollout and supervision of the regulations and policies of the Company's Governance and Sustainability System and of the governance and sustainability systems of the other companies of the Group, as well as any Guidelines approved in further development of these Foundations, to the extent they contain control frameworks regarding certain general risks for which certain main principles of conduct have been approved ("**specialist areas**").
- (iii) The risk division, which reports to the Internal Audit and Risk Division and is configured as an independent function, responsible for leading the design and implementation of the Comprehensive Risk Control and Management System for the identification and management of the material risks faced by the Group's companies.

## 6. Supervision of the Comprehensive Risk Control and Management System

The Company's Board of Directors is assisted by the Audit and Risk Supervision Committee, which, within the framework of its powers as a consultative body, monitors and reports on the effectiveness of the risk management and control system.

For the implementation and effective operation of the Comprehensive Risk Control and Management System, a Risk Committee has been created as a cross-functional, internal and permanent body made up of representatives from the Company's various corporate and business areas.

The Risk Committee shall supervise: (i) the adequate identification and management of the main risks within the risk appetite established by the Board of Directors; and (ii) the adequate operation of the internal reporting and control systems implemented for the management and control thereof.



## 7. Implementation and Monitoring

The Company's Internal Audit and Risk Division is responsible for the implementation of these Foundations and the achievement of their objectives, through the Risk Division (or such divisions as assume the respective powers thereof at any time), which will establish the necessary mechanisms for the coordination of the various actors in the Comprehensive Risk Control and Management System.

The Company's Internal Audit and Risk Division (or such division as assumes the powers thereof at any time) shall coordinate with the corresponding divisions of the other companies of the Group within their respective purviews. In particular, it relies on the support of the internal audit and risk divisions of the other companies of the Group, which handle the implementation and monitoring of the risk guidelines and limits.

\* \* \*

These Foundations, which were approved by the Board of Directors on 25 March 2025, include the content of the General Risk Control and Management Policy initially approved on 18 December 2007, which ceases to be in effect.