Doc. Ref.	POL-05	Version	1.0
Owner	Legal & Assurance	Effective Date	June 2024

Internal Control

Policy

MASORANGE Group

(This document has been translated from the current valid Spanish version for informational purposes only. If in doubt, please refer to the Spanish version)

Prepared by:	Reviewed by:	Approved by:
Internal Control, Risks and Compliance	Audit and Risk Committee	Board of Directors

Distribution List
- Public document

Version control

Version	Approval Date	Change from the last version
1.0	27/06/2024	*Initial Release*

Reference to other documents

Statutes and By-Laws of the Board
Code of Ethics
Anti-Corruption Policy
Crime Prevention Policy
Risk management and control policy

1. Index

2. Executive Summary

The Board of Directors of MASORANGE, S.L., is responsible for determining the policies and strategy of the Company and the companies that make up its group of companies ("Group") and in this regard decides to implement an Internal Control System based on best practices, integrated into daily activity and in which all areas of the company must participate.

3. Principles

In this sense, the COSO model developed by the *Committee of Sponsoring Organizations,* an organization dedicated to helping other organizations improve their performance through the development of leadership that improves internal control, risk management, governance and fraud deterrence, has been selected as a reference framework.

The COSO framework consists of five components:

- Control Environment
- Risk Assessment
- Control activities
- Information and communication
- Supervision

According to the 2013 COSO international standard adopted by MASORANGE, "internal control is a process implemented by the board, management and employees of an entity, intended to provide reasonable assurance as to the achievement of objectives related to operations, reporting and compliance."

4. Objective and scope

Objective

The objective of this policy is to establish the framework for the management of the Internal Control System that ensures the efficiency and safety of the processes.

In this sense, the Internal Control System must:

- comply with regulatory requirements in terms of internal control,
- provide reasonable security of financial and non-financial information support processes, and
- pursue the effectiveness and efficiency of operations and activities.

Scope

The policy applies to:

- all entities and activities of the Group,
- all employees and managers,

and covers risks that threaten:

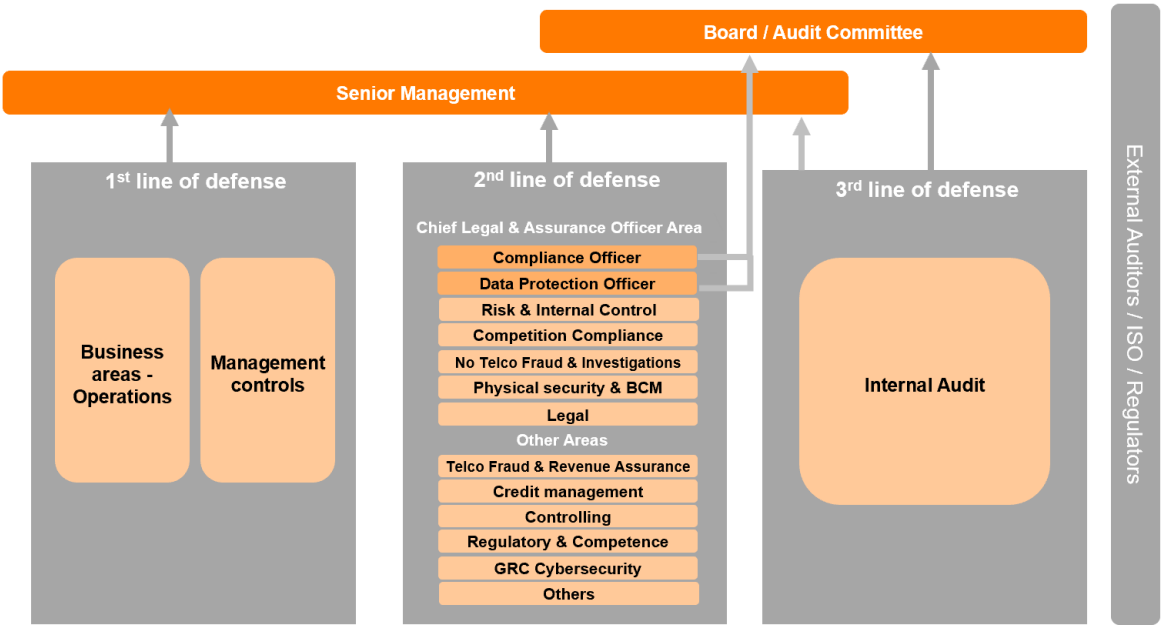
- the objectives of effectiveness and efficiency of operations;
- the reliability of information, and
- compliance with standards.

The policy is implemented through a risk-oriented Internal Control System of key processes, including those of information systems and services outsourced to third parties. Its scope is reviewed annually, taking into account both materiality and qualitative risk factors.

5. Organization & Responsibilities

Organization

The company implements its Internal Control System within the assurance model of the three lines of defense (IIA: Institute of Internal Auditors) in which each one acts at its own operational, supervisory and validating level:



- The first line is made up of the functions responsible for risk-taking processes. The first line includes, among other areas, Finance, IT, Network and Business units.
- The second line is made up of Internal Control, Risk and Compliance and other areas of the company that supervise effective risk control (DPO, Cybersecurity, Telco and non-Telco Fraud, Revenue Assurance, etc.).
- The third line is Internal Audit.

Responsibilities

The Group's control environment emanates from the governing bodies and senior management, which influence the rest of the organization through their own actions and behaviors, with the establishment of tools and controls that aim to cover the Group's significant risks.

A proper model requires a clear definition and communication of roles and responsibilities, ensuring adequate segregation of duties:

- Board of Directors. The existence and maintenance of the Internal Control System is promoted and monitored by the Board of Directors.
- Audit and Risk Committee. The Audit and Risk Committee is responsible for supervising the effectiveness of the company's internal control, as well as reviewing with the auditors the significant and material deficiencies detected in the internal control system. To this end, it is supported by the Internal Control function.
- Risk Committee. Its function is to coordinate the policies and actions of the different areas involved in risk control and management (second lines of defense). It carries out review activities in the application of essential elements of risk management (prioritization of main risks, risk appetite, risk methodology, risk assessment matrix, etc.), as well as informative meetings and monitoring of the evolution of the main risks, their controls, action plans and indicators. In addition, it can raise issues for the CEO/ Executive Commitee for its attention or suggestions in order to improve risk management or internal controls.
- Internal Control Working Group. The Risk Committee has an Internal Control Working Group responsible for monitoring internal control activities.
- First line. The first line is responsible for identifying and assessing risks to their processes and they are responsible for implementing and enforcing controls to mitigate them.
- Second line. The responsibility for the design, as well as the supervision of the implementation of the Internal Control System, falls on the Internal Control function with the support of the rest of the areas of the company. The Internal Control function, in collaboration with the rest of the functions of the second and third lines, will ensure the effectiveness of the Internal Control System.
- Human Resources Department. The Human Resources Department, in addition to having front-line responsibilities, is responsible for the design and review of the organizational structure and for regularly providing an updated organizational chart to the Internal Control function, which will maintain a record of the positions and persons with responsibility in the Internal Control System.

6. Governing Law

European Regulations

- Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC,

Directive 2006/43/EC and Directive 2013/34/EU as regards sustainability reporting by undertakings

U.S. Regulations

- Sarbanes-Oxley Act (SOX)

Spanish Regulations

- Law 2/2011, of 4 March, on Sustainable Economy
- Organic Law 5/2010, of 22 June, amending Organic Law 10/1995, of 23 November, on the Penal Code
- CNMV Guide: Internal control over financial information in listed companies
- Law 11/2018, of December 28, 2018, amending the Commercial Code, the revised text of the Capital Companies Law and Law 22/2015, of July 20, 2015, on Auditing of Accounts, in matters of non-financial information and diversity.
- CSRD (Corporate Sustainability Reporting Directive), the preliminary draft of the Sustainability Information Law for the transposition of this directive is in process.

7. Internal Control Framework

The main activities of the internal control system are:

- A scoping exercise is carried out annually that, through the analysis of the materiality of the headings of the financial statements and non-financial information, the identification of processes and systems with an impact on financial and non-financial information and the quantitative and qualitative factors of the associated risks, which allows the scope of the Internal Control System to be defined.
- The basis of the internal control system is the company's Control Environment, which is made up of governance rules, policies, committees, procedures and other standards that are grouped by processes. Each process has a process owner who annually conducts a self-assessment through a questionnaire designed by the Internal Control function in collaboration with the process leader.
- Key processes with a significant impact on financial and non-financial reporting have descriptive documentation that includes the risks and controls of each of them. This documentation is kept up-to-date by the functions responsible for processes (first line) and is monitored by the Internal Control function.
- The functions responsible for processes (first line) review annually that they have an adequate segregation of duties. This review is coordinated and overseen by the Internal Control function.
- The control activities that mitigate risks related to the financial statements and non-financial information are executed by the functions responsible for the processes (first line) and are formalized in a matrix of controls that is validated annually by each person in charge (*control owner*) and certified annually by its director. This certification is coordinated by the Internal Control function.

- On an annual basis, the Internal Control function carries out an evaluation of the functioning and effectiveness of the internal control system and is responsible for coordinating the external audit of the internal control system that is carried out within the framework of the audit of annual accounts and non-financial information.
- In the event that deficiencies are identified, they are reported to the Management of the responsible areas and to the Audit and Risk Committee. The Internal Control function monitors the action plans necessary to address these deficiencies.
- The Internal Control function will carry out or promote training actions on internal control focused on maintaining a strong internal control culture.

Likewise, the company has the following control elements:

- Limited power structure. The company has a detailed powers of attorney framework by scale of amounts and jointly and severally, which allows a limitation of the disposition of funds, contracting and representation.
- Code and Ethics Channel. A Code of Ethics is maintained, approved by the Board of Directors, which constitutes the reference framework in terms of the basic principles to which the companies that make up the Group and all its employees and administrators must abide in the development of their activities. In relation to the Group's financial and non-financial information, the Code of Ethics stipulates the obligation to: "*pay special attention to aspects related to the Internal Control Systems of Financial and Non-Financial Information in order to ensure the clarity and accuracy of transactions and their respective accounting records and the preparation of financial and non-financial information*".

  The Company has an Ethics Channel available to all Group employees which, among other purposes, is a transparent channel for reporting conduct that may involve the commission of an irregularity or an act contrary to the law or the rules of conduct of the Code of Ethics and internal regulations.

8. Review & Monitoring

This Policy is approved by the Board of Directors and shall enter into force on the day of its approval.

The application of this Policy will be subject, in any case, to the modifications that, in accordance with the legislation in force at any time or the interpretation of it made by the Company itself and that it deems appropriate to include.

The Board of Directors shall periodically evaluate the effectiveness of this Policy and shall adopt appropriate measures to remedy any deficiencies therein, making any modifications it deems appropriate.

9. Glossary of terms

Control/control activities. These are the activities that help mitigate the risks identified in each of the processes.

General controls of the entity. Controls that operate throughout the organization and generally have a present impact on controls at the process, transaction, or application level.

***Internal Control*.** A process developed by the Board of Directors, management and employees of the organization in order to provide a reasonable degree of assurance for the achievement of objectives related to operations, reporting and compliance.

***Control environment*.** A set of rules, processes and structures that emanate from the management of the organization and constitute the foundations on which internal control is developed at all levels of the organization.

Deficiency of control. Deficiency of internal control resulting from the absence of controls to ensure the reliability of financial information, its incorrect design or its operational inefficiency.

Material deficiency. Deficiency of control that implies a reasonable possibility of a material error in the information, both financial and non-financial.

Significant deficiency. Deficiency of control, less severe than a material deficiency, but relevant enough to merit the attention of the supervisors of the process of preparation and issuance of the information.

Error. Accidental or intentional act by which information is omitted or presented incorrectly, causing the information not to be presented in compliance with the preparation standards applicable to the organization.

***Risk assessment*.** The process of identifying and assessing risks that affect the reliability of financial and non-financial information.

***Fraud*.** Intentional act committed by one or more individuals of the company's management, employees, or third parties, including the use of deception to gain an illegal or unfair advantage.

Information and communication. Information systems identify, collect, process, and distribute information about transactions and events. Communication systems serve to distribute to the organization the criteria, guidelines, instructions and, in general, the information that the members of the organization must have in order to know their functions and the manner and time in which they should be performed.

Financial information. Content of the annual accounts, including the balance sheet, the profit and loss account, the statement of changes in equity, the statement of cash flows and the annual report, as well as the accounting data contained in the management reports.

Non-financial information. Sustainability report content or Non-Financial Information Statement (NFIS) which is the report used to communicate performance and strategies in

areas other than financial areas, such as the environment, social and corporate governance.

Materiality: The magnitude of an error or omission in financial and non-financial information that may change or influence a person's reasonable judgment.

Control Owner. An employee responsible for the execution and documentation of a certain control.

Risk: The possibility that an event will occur and adversely affect the reliability of financial and non-financial information.

***Segregation of duties*.** A control activity consisting of separating the responsibilities of the various activities involved in the preparation of financial statements and public information, in order to reduce the risk of errors, omissions or malpractices.

***Reasonable security*.** A high degree of assurance that the financial statements, as well as the non-financial information as a whole, are free from misstatement arising from fraud or error, based on the premise of risk management, no matter how well designed and operational, cannot provide a guarantee that the entity's objectives will be achieved; due to the inherent limitations of such management.

Internal Control System for Financial Reporting (ICFR). A set of processes that the Board of Directors, the Audit and Risk Committee, the management and the personnel involved in the entity carry out to provide reasonable assurance regarding the reliability of the financial information they disclose.

Internal Control System for Non-Financial Information (SCIINF). A set of processes that the Board of Directors, the Audit and Risk Committee, the management and the personnel involved in the entity carry out to provide reasonable assurance regarding the reliability of the non-financial information they disseminate.

***Supervision*.** A set of activities to verify that the internal control policies and procedures implemented to ensure the reliability of information (financial and non-financial) have been properly designed and are effectively operational, so that they can provide reasonable assurance that the system is effective in preventing, detecting and correcting any material error or fraud in public information.