ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Publicly-Held Company NIRE 35300010230

COMPLIANCE POLICY

SUMMARY
Establishes the fundamentals associated with the *Compliance* function (compliance).

1. OBJECTIVE
Establish the guidelines and main duties associated with the *Compliance* function, observing good market practices and applicable regulations.

2. TARGET AUDIENCE
Itaú Unibanco Holding and its subsidiaries in Brazil and companies abroad listed in internal procedure.

3. INTRODUCTION
The Compliance role aims to prevent and mitigate Itaú Unibanco's exposure to situations of non-compliance with standards and commitments (Compliance Risk), being responsible for governance, certification of adherence, conduct and transparency.
Regulatory Risk or Compliance Risk is the risk of sanctions, financial loss or reputational damage arising from failure to comply with legal and regulatory provisions, local and international market standards, internal policies, commitments to regulators, voluntary commitments in addition to self-regulation and conduct codes adhered to by Itaú Unibanco .
Compliance risk is managed through a structured process that aims to identify changes in the regulatory environment, analyze the impacts on the institution's departments and monitor actions aimed at adherence to regulatory requirements and other commitments mentioned in the previous paragraph.
Itaú Unibanco adopts the strategy of three lines of defense to operationalize its risk management structure, including *Compliance,* and to ensure compliance with the guidelines set out in this policy, with a clear division of roles and responsibilities.
The three lines work in a coordinated manner for the management of Compliance Risk in order to provide senior management with a global view of regulatory risk exposure.

3.1. First Line of Defense
It is represented by the Business and Support departments. Its employees are directly responsible for risk management and adherence to the rules associated with its operations, as well as for carrying out controls and implementing corrective measures for the proper handling of risks.

3.2. Second Line of Defense
It is represented by the departments responsible for risk control activities, which are fully segregated from the activities of the internal and legal audit, being independent in the exercise of their functions.
It has direct communication both with the administrators, including the members of the Board of Directors and the Audit Committee, as well as with any employee, and has access to any information necessary within the scope of its responsibilities.
In Brazil and abroad, the departments that make up the second line of defense are prohibited from managing any business or process that could compromise their independence or generate conflicts of interest. For the same reason, your goals and compensation cannot be related to the performance of the business departments.

3.3. Third Line of Defense
It is represented by the Internal Audit, which provides an independent assessment of the institution's activities, through auditing techniques, allowing management to assess the adequacy of controls, the effectiveness of risk management, the reliability of the financial statements and the compliance with standards and regulations.

4. GUIDELINES
As for the *Compliance function*
The management of compliance risks should address existing or new processes, products and services, including relevant outsourced services. Such processes, products and services must be periodically tested and evaluated for adherence to applicable standards, commitments made with regulators and requirements related to the Code of Ethics. To contribute to proper risk management, Itaú Unibanco has a risk management methodology comprising 5 stages: identification, prioritization, risk response, monitoring and reporting.

The Compliance role is coordinated and performed by the Corporate Compliance and Money Laundering Prevention Board (DCCPLD), reporting to the Risk Management Department (AR), and acting independently from the Conglomerate's other support and business departments. Additionally, under the coordination of DCCPLD, the Operational Risk Board, also reporting to the Risk Management Department, performs compliance functions in the coverage of Risks and Finance and Technology, through the certification of the control environment of the regulatory aspects of these departments, which occurs by prioritizing topics recorded in the Risk Maps and carrying out Operational Risk Diagnostics (DRO).
The AR aims to consolidate the risk culture and strengthen the management and governance of operational risks and of the organization's Compliance activities.
The non-compliance findings identified by any departments of the Conglomerate, regulators and other supervisory and inspection bodies must be monitored so that their effective treatment by the competent departments is guaranteed.
Compliance risk reports must be clear, objective, and timely, and must be reported to superior committees, business unit executives, the Risk executive, the Risk and Capital Management Committee, the Audit Committee and the Board Directors, so that the level of exposure and compliance with the established limits are monitored.
In the International Units, there are local and independent structures responsible for Compliance*,* under the responsibility of the local *Compliance Risk Officers* (CROs), who report the status of risks to the Regional CROs who, in turn, report it to the Global CRO, according to the organizational structure described in internal procedure.

5. MAIN ROLES AND DUTIES

5.1. Board of Directors

The Board of Directors is responsible for:
- Approving:
a) the guidelines, strategies and policies relating to *Compliance*, in order to ensure a clear understanding of the roles and responsibilities for all levels of the Conglomerate; and
b) the position of the DCCPLD in the organizational structure of the institution in order to avoid possible conflicts of interest, especially with the business departments.
- Provide the necessary means so that the activities related to the *Compliance* function are properly carried out, including the availability of resources to allocate sufficient personnel and with the necessary training and experience.
- Meet with the DCCPLD, at least annually, as part of the assessment of the effectiveness of compliance management
- Ensuring:
a) proper management of this policy;
b) effectiveness and continuity of the application of this policy;
c) communication of this policy to all employees and relevant outsourced service providers;
d) dissemination of standards of integrity and ethical conduct as part of the institution's culture; and
e) adoption of corrective measures for identified *Compliance failures.*
The evaluation of these items by the Board of Directors will be carried out on the basis of periodic meetings and the annual report prepared by the DCCPLD, as well as an annual evaluation carried out by the Audit Committee.

5.2. Audit Committee

The Audit Committee is responsible for:
- Validating the *Compliance* Policy prior to submission for approval by the Board of Directors.
- Evaluating, at least annually, the *Compliance* structure, in relation to the following aspects:
a) Clear definition of the duties, roles and responsibilities of the *Compliance* function, avoiding possible conflicts of interest, especially with the institution's business departments;
b) Positioning at an appropriate hierarchical level, independent and segregated from operational and business departments, with a duly exercised mandate regarding the definition of scope, execution of the work and communication of its results;
c) Organizational structure consistent with the needs of the Conglomerate and allocation of sufficient personnel, adequately trained and with the necessary experience to carry out the activities related to the respective functions;
d) Effectiveness of *Compliance* management; and
e) Adherence of the structure to the applicable regulation.
- Checking the performance of:
a) communication of this Policy to all employees and relevant outsourced service providers;
b) dissemination of standards of integrity and ethical conduct as part of the institution's culture; and
c) adoption of corrective measures for identified failures.

5.3. First Line of Defense

- Inform and train employees and relevant third-party service providers on matters relating to *Compliance.*

- Liaise with Regulatory, Self-Regulatory, Supervisory and Overseeing Agencies, responding to their requests, and issuing the appropriate reports to them, as established in the Policy on Relationship with Regulatory, Self-Regulatory, Supervisory and Overseeing Agencies;
- Identify, measure, evaluate and manage *Compliance* risk events that may influence the fulfillment of the Conglomerate's strategic and operational objectives;
- Maintain an effective control environment consistent with the nature, size, complexity, structure, risk profile and business model of the operations carried out, in order to ensure the effective management of *Compliance* risks, maintaining exposure to risks at acceptable levels according to the risk appetite established for the Conglomerate;
- Define and implement action plans to address non-compliance findings;
- Promptly communicate to the *Compliance* department whenever it identifies changes or non-compliance with current rules and regulations or *Compliance* risks not predicted by the control activities; and
- Maintain compliance with standards and regulatory requirements.

5.4. Second Line of Defense
Risk Management Department:
It is up to the Risk Management Department , through the DCCPLD and DRO:
- Supporting the first line of defense in observing their direct responsibilities.
- Disseminating integrity and ethical standards as part of the Conglomerate's risk and control culture and disseminating good practices and policies related to the *Compliance* function.
- Guiding and advising the Conglomerate's administrators and employees, directing specific solutions on compliance with internal rules related to the Integrity and Ethics Program;
- Guiding and advising the Conglomerate's administrators and employees, directing specific solutions related to compliance with external standards;
- Ensuring that the teams responsible for performing the *Compliance* functions have appropriate authority and that they are adequate, both in resources and knowledge, through a structured training program;
- Categorizing *Compliance* topics according to their severity and monitoring the conglomerate's exposure to these risks;
- Certifying the efficiency of *the First Line of Defense Compliance* control environment, through monitoring and testing programs, reporting the results to Senior Management and, when requested, to the Regulatory Agencies;
- Follow up investigations related to internal and external complaints, sanctions or supervisory measures applied by Susep or other authorities, among other cases that may signal risks to compliance;
- Reviewing and monitoring the action plans adopted to address the findings made by regulatory agencies;
- Reviewing and monitoring the action plans adopted to address the findings made by the independent auditor in the non-compliance report with legal and regulatory provisions;
- Reporting to the Executive Board, the Audit Committee, the Risk and Capital Management Committee and the Board of Directors the relevant situations that are not in compliance;
- Develop and disseminate to the IUs a script containing the best practices and Compliance methodology adopted by the Headquarters;
- Coordinating the implementation, monitoring and evolution of the Corporate Program for Integrity and Ethics in International Units; and
- Coordinating the governance of *Compliance* Programs of international regulations relevant to the conglomerate.

Exclusive roles of the DCCPLD are:

i. Defining principles and guidelines for disseminating the *Compliance* Culture, including training.
ii. Manage the process of capturing, screening, impact assessment and monitoring compliance with new regulations.
iii. Timely reporting relevant information both on the results of the *Compliance* assessments carried out that have identified material flaws and on significant changes in the regulatory environment.
iv. Managing the Integrity and Ethics Programs and Monitoring Abuse Practices (*Trade Surveillance*).
v. Coordinate the relationship with regulators and other supervisory and overseeing agencies with centralized management, monitoring the actions arising from the commitments assumed, facilitating the sharing of information and ensuring the consistency of the institutional positioning.
vi. Developing and making available the methodologies, tools, systems, infrastructure and governance necessary to support the *Compliance* function in the Conglomerate's activities.
vii. Coordinating the governance of Itaú Unibanco's policies and procedures, in accordance with applicable regulations, maintaining evidence of approval of all documents by the established approval authorities, including the approval of this Policy.
viii. Monitoring the Personal Investment Policies and the Securities Trading Policy issued by Itaú Unibanco Holding S.A.
ix. Sending to the Audit Committee and the Board of Directors an annual Compliance Report containing a summary of the results of activities related to *Compliance* topics, main conclusions, recommendations and action plans adopted to address identified deficiencies.
x. Monitoring the actions taken to report violations or red flags uploaded through the available reporting channels.

xi. Manage the Integrity and Ethics and Monitoring of Abusive Practices programs (*Trade Surveillance*), with operational support from the Capital, Market Risk and Liquidity (DCRML) Department.

In the International Units, the Local CROs are responsible for the above items according to the governance established in internal procedure.

5.5. Third Line of Defense

Independently and periodically verify the adequacy of risk identification and management processes and procedures, including the integrated management of operational risk, internal controls and Compliance, in accordance with the guidelines established in the Internal Audit Policy and submit the results of your findings to the Audit Committee.

5.6. Common to All Departments of Itaú Unibanco

- Conduct training on integrity and ethics and risk management provided by Itaú Unibanco.
- Annually sign the Term “Corporate Integrity Policies” attesting to its knowledge and agreement with what is established in this Policy.
- Define, implement and comply with policies and procedures for adherence to regulations.
- Comply with the provisions established by the Conglomerate's external rules and internal policies.
- Communicate fact or suspicion of violations of the Code of Ethics, the Integrity, Ethics and Conduct Policy or this policy.

6. RELATED EXTERNAL RULES

Basel Committee on Banking Supervision - Compliance and the compliance function in Banks (April 2005)
Resolution No. 4,968/21 of the Brazilian National Monetary Council: provides for the implementation and implementation of an internal control system
Resolution No. 4,557/17 of the Brazilian National Monetary Council: addresses the risk management structure and the capital management structure
Resolution No. 4,595/17 of the Brazilian National Monetary Council: addresses the compliance policy of financial institutions and other institutions authorized to operate by the Central Bank of Brazil.
Resolution No. 65/21 of the Central Bank of Brazil: addresses the compliance policy of consortium administrators and payment institutions.
Resolution No. 416/21 of the Brazilian National Private Insurance Council: provides for the Internal Controls System, the Risk Management Structure and the Internal Audit activity.

Approved by the Board of Directors on 2022, June.