COMPLIANCE AND INTERNAL CONTROLS POLICY

TABLE OF CONTENTS

1 PURPOSE

The purpose of this Policy is to set out concepts, rules and responsibilities governing the functioning of the Company's Compliance and Internal Controls structure.

2 SCOPE

This Policy applies to all administrators, employees and interns of B3 S.A. – Brasil, Bolsa, Balcão ("B3"), its subsidiaries abroad and in Brazil, BSM Market Supervision ("BSM"), Cetip Info Tecnologia S.A., B3 Social, and other associations in which B3 is a sponsor, honorary or founding partner ("Company").

3 REFERENCES

The references for this Policy are the main national and international normative instruments that deal with concepts, rules and responsibilities relating to the Compliance and Internal Controls structure, including:

- Anti-Corruption and Fraud Prevention Policy;
- Corporate Risk Management Policy;
- Brazilian Federal Law No. 4,595/1964;
- Brazilian Federal Law No. 4,728/1965;
- Brazilian Federal Law No. 6,385/1976;
- Brazilian Federal Law No. 10,214/2001;
- Central Bank of Brazil Resolution No. 304/2023 (BCB Resolution No. 304/2023);
- Brazilian National Monetary Council Resolution 4,952/2021;
- Brazilian Securities and Exchange Commission Resolution No. 135/2022; and

- SUSEP Circular Letter No. 599/2020.

4 CONCEPTS

4.1 Regulatory Environment

Is the set of legal, normative and regulatory provisions issued by the bodies that regulate the Company's activities.

4.2 Internal Control System

The set of procedures and activities established by the Company to reduce the likelihood of financial losses and damage to its institutional image, enhance the quality of its accounting information and assure compliance with the applicable legislation and regulations.

5 GUIDELINES

5.1 Implementation, Assessment and Maintenance of Internal Control Activities

The Governance, Integrated Management and Cybersecutiry Department is responsible for assessing and monitoring whether the control activities: (i) are being carried out by the Company's operating areas and (ii) are sufficient, effective and efficient in mitigating risks.

Control activities are assessed from time to time based on the legislation and regulations in force and on best practices in Corporate Governance, embodied in the standards and methodologies established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Control Objectives for Information and Related Technology (CobiT) framework.

The results of assessments and tasks are duly documented and forwarded to the operating areas responsible for control activities.

Internal control activities must be properly documented by business area managers. The nature and extent of this documentation may take various forms, containing at least:

- Duly formalized policies and procedures;
- Formalization of the responsibility of each professional involved in the relevant business processes, with the appropriate segregation of functions and approval authorities, where applicable. This formalization may take the form of organization charts, responsibility matrices, job descriptions and/or narratives; and
- Supporting documentation for decisions taken regarding the implementation of controls, including cost-benefit assessments.

In addition, the Governance, Integrated Management and Cybersecurity Department is responsible for complying with the requirements of the Central Bank of Brazil, particularly in respect to BCB Resolution No. 304/2023, and with external auditors in matters relating to the assessment of the Company's control environment.

To this end, business areas must provide the requisite information to the Governance, Integrated Management and Cybersecurity Department so that it can produce reports on internal controls for approval by the Board of Directors.

5.2 Action Plan Follow-up

Concerns resulting from the assessments of external and internal audits, of regulatory bodies or second line areas (Corporate Risks, Compliance, Internal Controls, Business Continuity, Crisis Management, Financial Risk, and Information Modeling and Security) shall be validated by the business areas, which are responsible for producing and executing action plans to address deficiencies and noncompliance.

The Governance, Integrated Management and Cybersecurity Department shall test the deployment of plans when completed, in accordance with the Internal Controls methodology, except those resulting from concerns raised by internal audit, which will be reviewed by the auditors themselves.

Changes to the duration of action plans due must be submitted for approval according to their risk classification and clearance level, as contemplated by the Internal Audit Rule and the Corporate Risk Management Policy.

When the structure of an area does not include the required level of clearance, an approval request must be submitted to the next hierarchical level.

Changes to the duration of action plans due to concerns of internal auditors, as described above, must be conveyed to the Audit Department, which reports semiannually to the Audit Committee and the Executive Board on all action plans completed and redesigned in the period.

The Governance, Integrated Management and Cybersecurity Department shall notify the competent clearance holders, as defined in the Control Activities Assessment Methodology, of expired action plans devised by areas that did not (i) report their effective implementation or (ii) submit a request for their redesigning within the stipulated duration.

5.3 Regulatory Environment Monitoring

The purpose of regulatory environment monitoring is to identify the issuance of new regulations or changes to existing regulations that apply to the Company, so that the necessary adaptations can be made to ensure compliance.

Compliance with the rules and regulations issued by the National Monetary Council, Central Bank of Brazil (BCB), Brazilian Securities & Exchange Commission (CVM), Superintendence of Private Insurance (SUSEP) and

the National Traffic Secretariat (Senatran), which regulate the Company's activities, is verified, monitored and analyzed by the Governance, Integrated Management and Cybersecurity Department, jointly with the business areas affected.

If rules and regulations issued by other bodies create obligations for the Company, they shall be monitored by the specific areas involved.

The Governance, Integrated Management and Cybersecurity Department

periodically reports to the Executive Board on the applicable rules and regulations, on the Company's compliance with them and on the adoption of action plans to comply with them, where applicable.

5.4 Access to Premises

The Governance, Integrated Management and Cybersecurity Department has full access to the Company's premises and controlled access to security areas, where the Department's professionals must be met and accompanied by the staff responsible for the relevant sector, and logical access to information.

5.5 Access to Information and People

The Governance, Integrated Management and Cybersecurity Department has full access to digital and logical information and the staff covered by this Policy. All information obtained must be treated as confidential.

6 RESPONSIBILITIES

6.1 Board of Directors

- Approves the Company's Internal Control reports after review and opinion by the Audit Committee.

6.2 Audit Committee

- Oversees the activities of the Company's Internal Controls area;
- Monitors the quality and integrity of the Company's Internal Control mechanisms, and recommends improvements to policies, practices and procedures;
- Assesses the effectiveness and sufficiency of Internal Control systems on legal, tax and labor risks; and
- Reviews reports on the Company's Internal Controls prior to their discussion by the Board of Directors.

6.3 Executive Board

- Conducts business practices that comply with the legislation and regulations applicable to the Company and with its internal policies, rules

and procedures;

- Sponsors the implementation of efficient business practices and adequate and effective internal controls, allocating the necessary resources and defining the appropriate infrastructure for internal control system management;

- Monitors the execution of action plans and approves their redesigning (duration) in relation to (i) risk management; (ii) internal and external audits, and inspections by regulators; (iii) risk mapping and assessments by internal controls and compliance teams; and

- Assures the autonomy of the Governance and Integrated Management Department to perform its activities, guaranteeing access to documents, information systems and people, and the sharing of reports, correspondence and other information required for the performance of the Department's activities.

6.4 Governance, Integrated Management and Cybersecurity Department

- Assures compliance with and dissemination of this Policy;
- Defines and applies the methods used to assess and monitor the Company's internal control system;
- Complies with the Central Bank of Brazil's requirements, particularly in respect to BCB Resolution No. 304/2023, and with external auditors in matters regarding the assessment of the Company's control environments;
- Monitors the regulatory environment and oversees the execution of action plans to ensure compliance with regulatory provisions;
- Participates in discussions on projects or changes to normative documents submitted to public hearings or consultations, whenever such proposals affect the Company's regulatory matrix;
- Helps business areas analyze their structures, products and services in order to align them with the rules and regulations issued by regulators and the Company;
- Monitors the execution of action plans and reports on their status (progress and redesigning) to the Executive Board; and
- Assists the Company in maintaining an effective internal control system, consistent with the nature, size, complexity and risk profile of the operations performed by B3 with a focus on:

  (a) Operational efficiency and effectiveness;

  (b) Integrity of data and information records;

  (c) Conformity; and

  (d) A risk-based approach.

6.5 Legal Department

- Provides legal advice to the Governance, Integrated Management and Cybersecurity Department and to the business areas on the legislation and regulations applicable to the Company and its activities;
- Participates in the production and amendment of the Company's normative documents; and
- Coordinates internal discussions on proposed changes to normative documents when these are submitted to public hearings or consultations.

6.6 Business Areas

- Manage the risks and control activities associated with the processes and systems under their management;
- Establish, maintain, promote and evaluate efficient business practices, as well as adequate and effective internal controls;
- Document their own internal controls;
- Provide, in a timely manner, the information required for the assessments of the Company's compliance with the regulatory framework and for the production of internal control reports;
- Act on the concerns arising from the work carried out by the risk, internal controls, compliance and audit teams, and inspections by regulators;
- Describe action plans, naming the person responsible and specifying the implementation date for each plan; and
- Assure the execution of action plans in accordance with the defined description and duration, requesting permission for duration and/or scope redesigning from the competent authority.

7 FINAL PROVISIONS

The above provisions apply to the entire Company upon publication of this Policy.

8 CHANGE LOG

Validity: As of March 20, 2025.

1st draft: April 4, 2013.

Areas responsible for the document:

Responsible for	Area
Drafting	Corporate Internal Controls and Compliance Department
Revision	Governance, Integrated Management and Cybersecurity Department Corporate Governance and Nomination Committee Audit Committee
Approval	Executive Board Board of Directors

Updates:

Version	Changed section	Reason	Date
1	Principles included	Completion of conceptualization	April 30, 2014
2	Bullet item “Assuring independent, impartial and timely internal auditing of the internal control system” excluded	Item included in Audit Committee Internal Regulation	
	Prerogatives included	Access by the Corporate Internal Controls Department to all inputs required for the performance of its duties	
	Inclusion of Corporate Risk Management Policy and Operational Risk Policy	References	

3	Inclusion of CobiT methodology as a reference to good practices	References	
	Inclusion of Compliance Policy	References	
	Managers' titles changed	Adjustment to Company's new standards	
4	Compliance Policy and monitoring of regulatory environment included Independent assessment of internal control system by Audit Department excluded Follow-up of action plans included	Project B3Together	June 28,2017
5	Formatting adjusted Wording of normative references improved Internal Controls and Compliance Department's responsibilities enhanced Corporate Internal Controls Department's activities adjusted Audit Department's responsibility included Business areas' responsibilities enhanced Legal Department's responsibilities adjusted Reporting of doubts on Policy's applicability to Internal Controls and Compliance Department included	Company's corporate restructuring	December 12, 2019
6	Scope and formatting	Adjustment to new governance of the Company's subsidiaries Alignment with new template	August 17, 2020

7	Concepts Guidelines Responsibilities	Exclusion of risk concept, as the updated concept is already included in the Corporate Risk Management Policy Update of activities under the internal controls area's responsibility Inclusion of information about documentation and delivery to operating areas of assessments conducted on control activities Rearrangement of parts of the text	June 25, 2021
8	References Guidelines Responsibilities	General wording review to adjust to BCB Resolution No. 174	March 31, 2023
9	References Guidelines	Regulatory update Update of the Reference Update of the nomenclature of the Governance, Integrated Management and Cybersecurity Department Update of the topic "Implementation, Assessment and Maintenance of Internal Control Activities" to exclude the item business process flowcharts as a minimum documentation requirement. Update of the topic "Monitoring of Plans" to remove redundancy and maintain the reference with the Corporate Risk Management Policy and the Internal Audit Regulations.	March 20, 2025