Table of contents:

01. PURPOSE

This policy is part of the continuous and integrated risk management structure of the Financial Conglomerate BOCOM BBM ("BOCOM BBM") and aims to present a set of principles and guidelines that must guide BOCOM BBM's **Operational Risk** control and management strategy.

02. CONCEPT/DEFINITION

02.01. **Operational risks**

Pursuant to article 32 of Resolution No. 4.557, of 2017, Operational Risk is the possibility of direct or indirect loss, resulting from external events or from deficiency, inadequacy or failures of internal processes, people or systems. In addition to the definition of operational risk, there is the legal risk associated with inadequacy or with inadequacy or deficiency in contracts signed by the institution, sanctions for noncompliance with legal provisions and compensation for damage to third parties resulting from activities developed by the institution.

02.02. **Operational Risk Categories**

In recent years, Operational Risk has become more complex, as its number and diversity of types has increased. The main categories managed by BOCOM BBM are:

02.02.01. Internal Frauds

Losses caused by acts with the intention of defrauding, misappropriating or circumventing regulations, laws or company policies, which involve at least one internal party, excluding diversity / discriminatory events.

02.02.02. External Frauds

Losses caused by acts intended to defraud, misappropriate, or circumvent laws, committed by a third party; They may include money laundering, identity theft and misrepresentation of assets or revenue.

02.02.03. Employment disputes and poor workplace safety

Losses due to inadequate / ineffective recruitment of personnel, lack of talent management, training and or high turnover. It also considers losses arising from acts that are inconsistent with employment contracts or laws, health, safety, payment of claims for bodily injuries, or from diversity/discriminatory events.

02.02.04. Inappropriate practices regarding final users, clients, products, and services

Losses arising from an unintentional or negligent failure to fulfill a professional obligation to specific clients (including fiduciary requirements and suitability to the client's profile), or the nature or design of a product or service. They may include missed deadlines or lost project budgets, as well as missed / incomplete and / or poor-quality deliveries.

02.02.05. Damage to physical assets owned or in use by the Institution

Damage related to losses or damage to physical assets (facilities) caused by natural disasters or other events (e.g. human action);

02.02.06. Interruption of the institution's activities or discontinuation of the services provided

Losses resulting from business disruption, caused by the absence or non-provision of essential services, whether from internal or external agents to the company.

02.02.07. Failures in systems, processes or information technology (IT) infrastructure

Losses resulting from failures in the Information Technology system or infrastructure resulting from internal (backup failure, systems unavailability, among others) or external (poor performance of the service provider, effects of nature, among others) facts.

02.02.08. Failures in execution, meeting deadlines and managing activities (process failures)

Losses arising from the administration, conduction, execution, and management of activities linked to internal business processes of the Institution.

02.02.09. Damage to Information Security

Loss due to theft, improper access, or leakage of personal or sensitive data. It includes losses associated with unauthorized access to systems whether due to the absence of segregation, through *hacking*, or damage to systems, among other reasons.

02.03. **Risk factors**

- People: relate to the skills, ethical conduct and performance of their duties;
- Processes: Flows and stages in the development of products and services and performance of the organization's activities, establishment of internal regulations and compliance with legislation;
- Technology: Systems, Infrastructure and IT architecture, availability of storage, processing and network;
- External: Related to the occurrences of the environment, the country's regulatory environment and the social environment (related parties, with the main example: service providers).

02.04. **Operational Loss**

Pursuant to paragraph 1 of article 34 of Resolution No. 4.557 of 2017, operational loss is defined as the quantifiable amount associated with the operational risk events mentioned in item 02.01 e 02.02. Those associated with credit risk, market risk, social risk, environmental risk and climate risk must be included in the operational risk database, regardless of whether they are also included in other databases.

02.04.01. Actual Loss

The effective loss results from an operational risk event that caused a financial or accounting loss to the company, directly affecting its result.

02.04.02. Ineffective or Potential Loss

Situation in which the operational risk events did not cause an effective loss to the company, due to the intervention of an internal or external agent before the loss.

02.05. **Operational Incident**

Occurrence of non-compliance events associated with operational risks (as defined in 02.01 in e 02.02), originating in one or more risk factors (as defined in02.03) and may or may not affect operational losses (as defined in 02.04).

02.06. **Relevant Operational Incident**

Operational incident that:

- caused or could cause relevant financial losses;
- affected or could significantly affect business processes;
- caused or could cause damage to sensitive data or information or even have a significant impact on our clients or the Institution's image.

On the Internal Controls area intranet, we publish criteria for guidance as to the relevance of an operational incident.

02.07. **Cyber Risk**

It is a subcategory of information security risk, explained in item 02.02.09, but given its relevance, it is sometimes treated separately. It represents the possibility of losses resulting from cyber incidents.

02.08. **Cyber Incidents**

Event related to the cyber environment that: a) has an adverse effect or poses a threat to the information technology (IT) systems or to the information that those systems process, store or transmit; or b) violates security policies or procedures regarding IT systems.

02.09. **Relevant cybersecurity incident**

Incident that affects critical business processes, or sensitive data or information, and has a significant impact on clients.

02.010. **Business Continuity Management**

It consists of a set of strategies to ensure the continuity of the institution's activities and limit losses resulting from the interruption of critical business processes. The following are part of the strategic continuity management:

- The Business Continuity policy in order to establish the organizational structure and the main guidelines and rules;
- Business continuity plans that establish procedures and estimated deadlines for restarting and recovering activities in the event of interruption of critical business processes, as well as the necessary communication actions; and
- Business Impact Analysis (BIA), to identify the main critical processes and the assets that support them, determine the main factors for implementing emergency plans and ensure that the main systems are restored first in the event of an interruption.
- Tests and reviews of business continuity plans at appropriate intervals.

03. SCOPE/AREAS INVOLVED

03.01. Scope of the Risk Structure

The risk management structure must be:

- Compatible with the business model, the nature of the transactions and the complexity of BOCOM BBM's current products, services, activities and processes;
- Proportional to the size and exposure of risks, as determined by the institution in the Risk Appetite Statement;
- Adequate to the risk profile and systemic importance of BOCOM BBM; and
- Able to assess risks arising from macroeconomic conditions and from the markets in which BOCOM BBM operates.

In addition, it must be suitable to the Bank's classification segment, pursuant to art. 2 of Resolution No. 4,553, of 2017 of the Central Bank, to which the Bank currently falls. The information described is adequate for Segment 3 (S3). If BOCOM BBM falls within Segment 1 (S1) or Segment 2 (S2), this document must be revised.

BOCOM BBM's operational risk management framework must provide for:

- policies establishing criteria for deciding on the outsourcing of services and the selection of their providers, including the minimum contractual conditions necessary to mitigate operational risk;
- implementation of an IT governance framework consistent with the risk appetite levels established in the RAS;
- IT systems, processes, and infrastructure that:
  - Ensure the integrity, security and availability of stored, processed or transmitted data and the information systems used;
  - Contain mechanisms for the protection and security of networks, electronic sites, servers and communication channels with a view to reducing vulnerability to digital attacks;
  - Adopt procedures to monitor, track and restrict access to sensitive data, networks, systems, databases and security modules;

- Monitor data security breaches and end-user complaints in this regard; It is
- Are adequate to the needs and changes in the business model, both in normal circumstances and in periods of stress;

03.02. **Policy Scope**

The policy applies to the Conglomerate BOCOM BBM and its STAKEHOLDERS. STAKEHOLDERS are employees, interns, shareholders, clients, other parties, suppliers and the communities in which we operate.

03.03. **Organizational Structure**

The operational risk management structure comprises the Risk Committee, the Operational Risk Committee and Internal Controls and the Risk, Internal Controls, and Information Security areas.

In addition, Compliance and Internal Audit, in an independent, autonomous and impartial manner, work to assess the quality and effectiveness of the systems and processes of internal controls, risk management and corporate governance of the institution of BOCOM BBM.

04. RESPONSIBILITIES

04.01. **Responsible for carrying out the duties of this policy**

As for execution, the units below have the following responsibilities:

04.01.01. Board of Directors / Risk Committee / Executive Board

- Approve annually the operational risk management policy for the institutions of BOCOM BBM;
- Establish BOCOM's operational risk appetite levels in the RAS; and
- Take strategic decisions to control the Operational Risk.

04.01.02. Operational Risk and Internal Controls Committee

- Disclose the risk management-oriented culture;
- Establish roles and responsibilities for each member of the Operational Risk structure;
- Inform the Risk Committee about the fulfillment of its recommendations and inquiries about the proper functioning of the operational risk management system;
- Analyze the relevant incidents that have occurred, and if necessary, decide actions to be taken in order to mitigate risks incurred;
- Assess the levels of appetite for operational risk established in the RAS and the strategies for management thereof;
- Analyze relevant situations of exposure of the institution to operational risks, proposing necessary adjustments to the organization; and
- Analyze situations not provided for in this policy.

04.01.03. Internal Controls

- Propose an operational risk management policy and suggest changes when necessary to be approved by the Board of Directors and the Executive Board;
- Disseminate the culture of operational risk awareness, to ensure that all employees are fully aware of the importance of operational risk management.

Regarding macroprocesses and processes:

- Identify, together with the business areas, each macroprocess/process existing in BOCOM BBM;
- Seek to develop, together with the managers of the areas, procedures containing the description of the (macro) processes and identify operational risks inherent therein and respective controls;
- Seek to establish, together with the managers of the areas, the key risk indicators;
- Assess the potential effects of the operational risks to which BOCOM BBM is exposed and report its conclusions internally and externally, when necessary;

Assessments are prioritized and are often carried out when:

a. A relevant operational incident occurred at the bank or at other banks;
b. The Bank's exposure to a relevant operational risk was identified;
c. There are significant changes in the procedures of a transaction;
d. There are significant changes to the operating systems;
e. When new products are launched;
f. When regulation with a relevant impact is issued or updated;
g. At the request of the regulatory body or the executive board.

With respect to operational risk events:

- Manage the database of records of operational risk events;
- Periodically monitor the operational risks identified to verify if any mitigators adopted are being effective and/or if there is an increase in the frequency of incidents related to these risks;
- Prepare reports to evaluate the relevant operational incidents, identifying the controls established to correct identified and any operational losses;

Regarding outsourced processes:

- Identify the risks and controls existing in the processes whose services are outsourced; and
- Keep the Supplier Selection, Contracting and Management Policy up-to-date with regard to the decision criteria regarding outsourcing services and selecting its providers, including the minimum contractual conditions required to mitigate the operational risk.

Regarding operational continuity:

- Business continuity management, contemplating the strategies to be adopted to ensure contingency conditions for the most critical activities and mitigate serious losses resulting from operational risk;

Regarding Regulatory reports:

- Together with the Compliance area, forward reports to the management bodies and for availability to the CVM, until the last business day of April of each year, containing the operational risk events, as well as their risk assessment and progress/completion of possible mitigators;
- Together with the Compliance area, report any Relevant Incidents regarding Cybersecurity, in accordance with the deadlines and audiences laid down in current regulations and internal policies. Incidents must be reported to BSM on a monthly basis.

Regarding the limits established in the RAS:

- Responsible for calculating, evaluating, reporting the of operational risk indicators and information technology indicators present in the RAS and, when necessary, bringing these indicators back around the target limit. The description of the indicators, as well as the calculation and monitoring are described in the Risk Appetite Management procedure.

04.01.04. Information Technology

- Provide the necessary technological support for the development of operational risk monitoring and control.

04.01.05. Information Security

- Assist, in synergy with the Internal Controls area, in the integrated identification of risks to the Institution;
- Analyze cyber risk incidents by informing the Risk Committee of any mitigating actions or impacts on the Institution's processes.
- Carry out a review of security and data confidentiality measures, especially after the occurrence of failures and prior to changes in infrastructure or procedures;
- Carry out tests to ensure the robustness and effectiveness of the data security measures adopted;
- Prepare reports that indicate procedures for correcting identified flaws;

04.01.06. Process managers

- Maintain awareness of the risks inherent in its processes, assessing them as to the probability of occurrence and their possible impacts;
- Assist in the preparation of process mappings;

- Inform about changes in processes, routines and controls that may cause, from time to time, changes in the assessment of risk exposure;
- Business management observing top management guidelines, such as the definition of Risk Appetite; and
- Disseminate the culture of operational risk awareness, to ensure that all employees are fully aware of the importance of operational risk management.

04.01.07. Other employees of the Institution

All employees must, when occurrences related to operational risks are identified, communicate them immediately to the Internal Controls area for the appropriate measures.

04.02. **Responsible for monitoring the execution of the duties of this policy**

The Manager of the Internal Controls area must monitor the execution of the duties of this policy.

04.03. **Responsible for maintaining this policy**

The Internal Controls area must maintain this policy.

05. AUTHORITIES

The Operational Risk and Internal Control Committee, the Executive Board and the Board of Directors must approve this policy.

The Operational Risk and Internal Controls Committee must analyze situations not provided for in this policy and assess whether it will be necessary for approval by the Board of Directors.

06. GUIDELINES:

06.01. **Principles**

06.01.01. Best Practices

The Internal Controls area, responsible for managing operational risk, analyzes and monitors the best control practices to be adopted to ensure the safety and reliability of processes.

06.01.02. Integrated Risk Management

Once an operational risk is identified, the Internal Controls area must seek to analyze the possible effect under other risks that the Bank manages. Currently the main risks that BOCOM BBM seeks to measure, evaluate, monitor, report, control and mitigate are:

- credit risk;
- market risk;
- liquidity risk;
- strategic risk;

- reputational risk;
- information security risk;
- regulatory risk;
- social risk
- environmental risk;
- climate risk; and
- operational risk, as provided in this policy.

Risk management must be integrated, enabling the identification, measurement, evaluation, monitoring, reporting, control and mitigation of adverse effects resulting from interactions among the risks mentioned.

06.01.03. Information Transparency

The description of the operational risk management structure is evidenced in this policy, which is available on the Bank's institutional website.

06.01.04. Risk Oriented Culture

The culture of operational risk management is disseminated in all areas of the institution as well as to our related parties. Whenever possible, training should be carried out to reinforce the importance of managing operational risks.

06.02. **Operational Risk Management Phases**

The operational risk management process of BOCOM BBM is methodologically divided into two phases: Preventive and Reactive.

06.02.01. Preventive Phase

Objective

This phase aims to identify operational risk events before they occur and create methods to avoid, mitigate, transfer or accept risk.

Steps

It consists of the following steps:

I. Identification: identify operational risk events, pointing out the areas of impact, causes and potential financial impacts.
II. Assessment: quantify the exposure to operational risk in order to assess the impact on the business.
III. Control: record the behavior of operational risks, limits, indicators and events of operational loss, as well as implement mechanisms in order to ensure that the limits and indicators of operational risk remain within the defined levels.

IV. Mitigation: create and implement mechanisms to mitigate operational risk, seeking to reduce losses.
V. Monitoring: identify deficiencies in the operational risk management process.

Tools

Examples of tools that help mitigate operational risks in the preventive phase:

- Establishment of Policies and Codes of Ethics and Conduct;
- Process Mapping and preparation of flowcharts;
- Formalization of operational manuals;
- Training;
- Monitoring;
- Implementation of (physical and logical) access controls, installation of antivirus programs, periodic data backup;
- Continuity Tests;

among others.

06.02.02. Reactive Phase

Objective

Treatment of operational risk events that have already occurred, whether or not they occurred in operational losses.

General Steps

I. Receipt of the Incident Report;
II. Analysis of its causes and impacts on business processes;
III. Identification of the event with other types of risk (e.g. cyber or social and environmental risk);
IV. Guidance on the actions that should be taken for the short-term solution and to prevent new incidents from occurring.

06.03. **Incident Report**

06.03.01. Who can make an incident report?

In the event occur, any employee can report it via an electronic form, available in the browser of all employees. Every incident will be subject to the assessment/approval of the manager of the reported area and the risk classification by the manager of the impacted area.

06.03.02. Incident Database

For each incident report, the following information must be stored:

- The internal code for identifying the operational risk event;
- The operational risk category, according to item 02.02.

- The risk factors, according to item 02.03, indicating the name of the process, system or external factor.
- The identification of the business unit in which it occurred, according to Annex I, item 014.01 of this policy;
- The dates of occurrence and discovery;
- The description of the event that occurred, whenever possible, informing the root cause;
- The short-term solution;
- The mitigating controls to prevent the event from occurring again;
- The impacted areas;
- The impacted processes;
- The accrued gross loss (when applicable);
- The accrued amount of the loss recovered by insurance or other means (when applicable);
- The source of the reimbursement, for loss recovery events (when applicable);
- The indication, based on consistent and verifiable criteria, of Category Level 1 and Category Level 2 in which the operational risk event falls, according to Annex II of this Circular Letter;
- The association, when applicable, to the other types of risk to which the Bank is subject: credit risk; market risk; social and environmental risk; liquidity risk; regulatory risk; reputational risk and cyber risk.

06.03.03. Loss Treatment

Operational risk losses occurred in the form of expenses will be considered for the formation of the internal losses database.

06.03.04. Request for additional information

After registration in the Internal Controls database, incidents will be analyzed and their root causes will be identified.

Note that in addition to Internal Controls, the Risk, Information Security, Internal Audit areas and the Operational Risk and Internal Controls Committee are also notified of the incident report. And each of these centers can request more information, if deemed necessary, either from those involved in the event or from the employee who made the report.

06.04. **Fraud Reporting**

BOCOM BBM is committed to repudiating any and all forms of fraudulent activity on the part of its employees, service providers, agents and brokers. Fraudulent activity means forgery, embezzlement, theft, personal use of assets, solicitation of a bribe or giving bribe to a public officer), misappropriation, questionable payments and receipts, misconduct in (public) office, among others.

Always thinking about the objective of providing good results, with total reliability, security and transparency, frauds must be reported to the *Compliance* Management so that it starts the relevant

investigations. Note that, due to their sensitive content, suspicions of fraud will be treated as confidential.

06.05. **Relevant Security Incidents**

Once an incident of damage to information integrity, data leakage or cyber-attacks has been identified, the Internal controls area must alert the Information Security area. This area is responsible for submitting these events to the Information Security Committee and monitoring any established treatments. The role of the Information Security area is to reaffirm our commitment to confidentiality, authenticity, integrity and availability of sensitive data and information and for taking measures to reduce our exposure to cyber-attacks.

Security incidents considered relevant must be reported to the Central Bank and the SMI (Commission of Market Relations and Intermediaries).

06.06. **Incidents putting the Business Continuity Plan in place**

Any event that has put the business continuity plan in place must be reported to the management bodies and to the Commission of Market Relations and Intermediaries (SMI).
The report must understand the causes of the plan being put in place, indicating the critical processes affected. In addition, the mitigators adopted or intended to be adopted, time consumed in solving the event and any other relevant information.

07. FINAL CONSIDERATIONS

This document is strictly for internal use and should not be made available to third parties without consulting the Internal Controls area manager.

08. RELATED LEGISLATION/REGULATION

- PQO, dated January 02, 2025;
- CMN Resolution No. 5.076, dated May 18, 2023;
- CMN Resolution No. 4.557, dated February 23, 2017;
- BCB Resolution No. 3.979 dated January 30, 2020;
- BCB Normative Instruction No. 33 dated October 29, 2020;
- BCB Normative Instruction No. 356 dated November 28, 2023;
- CMN Resolution No. 4,893 dated February 26, 2021;
- CVM Resolution No. 35 dated May 26, 2021;
- CMN Resolution No. 4,943 dated September 15, 2021; and
- CMN Resolution No. 4,968, dated November 25, 2021.

09. INTERNAL REFERENCE

- Risk Appetite Statement;
- Internal Controls Policy;
- Market Risk Management Policy;
- Credit Risk Management Policy;
- Liquidity Risk Management Policy;
- Operational Continuity Management Policy;
- Capital Management Policy;
- Information Disclosure Policy
- Data Protection Policy;
- Information Security Policy;
- Backup and Restore Policy;
- Product Approval Policy; and
- Process Evaluation Policy.

010. BIBLIOGRAPHY

- COSO 2017;
- Sound Practices for the Management and Supervision of Operational Risk;
- International Convergence of Capital Measurements and Capital Standards (Basel II);
- International Regulatory Framework for Banks (Basel III);
- Operational Risk Policies and Procedures of Bank of Communications.

011. GLOSSARY

- Bacen - Central Bank of Brazil;
- RAS: Risk Appetite Statement.

012. VERSION CONTROL

Version	Date	History	Authors
1.	06/27/2007	Document Creation	Operational Risk
2.	12/10/2008	Document Revision	Operational Risk
3.	12/14/2009	Document Revision	Operational Risk
4.	12/31/2010	Document Revision	Operational Risk
5.	12/13/2011	Document Revision	Operational Risk
6.	12/03/2012	Document Revision	Operational Risk
7.	12/04/2013	Document Revision	Operational Risk
8.	12/13/2014	Document Revision	Operational Risk
9.	12/29/2015	Document Revision	Operational Risk
10.	12/30/2016	Document Revision	Internal Controls and Operational Risk
11.	12/26/2017	Document Revision	Internal Controls and Operational Risk
12.	03/27/2018	Document Revision	Internal Controls and Operational Risk
13	12/31/2018	Document Revision	Internal Controls and Operational Risk
14	12/31/2019	Document Revision	Internal Controls and Operational Risk
15	01/31/2021	Document Revision	Internal Controls and Operational Risk
16	01/31/2022	Document Revision	Internal Controls and Operational Risk
17	01/31/2023	Document Revision	Internal Controls and Operational Risk
18	08/02/2023	Document Revision	Internal Controls and Operational Risk
19	02/01/2024	Document Revision	Internal Controls and Operational Risk
20	02/01/2025	Document Revision	Internal Controls and Operational Risk
21	09/06/2025	Document Revision	Internal Controls and Operational Risk

013. APPROVALS

_____

Tatiana Ferro– General Manager of Internal Controls and Operational Risk

_____

Monique Verboneen – Chief Risk Officer

014. ANNEXES

014.01. **Business Unit**

Corporate Finance
Negotiation and Sales
Retail
Commercial
Payments and Settlements
Financial Agent Services
Asset Management
Retail brokerage

014.02. **Operational Risk Categories**

Level 1	Level 2
Internal Frauds	Theft and fraud (internal origin)
	Unauthorized activity

Level 1	Level 2
External Frauds	Theft and fraud (external source)
	Systems security
	Other types of fraud of external origin

Level 1	Level 2
Employment disputes and poor workplace safety	Labor Relations
	Diversity and Discrimination
	Workplace safety

Level 1	Level 2
Inappropriate practices regarding clients, products and services	Adequacy of product to client, disclosure of information about products and services, failure to perform fiduciary duty
	Improper business and market practices
	Product failures
	Selection, sponsorship and exhibition
	Advisory activities

Level 1	Level 2
Damage to physical assets owned or used by the institution	Disasters and other events

Level 1	Level 2
Situations that cause the interruption of the institution's activities;	Interruption of activities

Level 1	Level 2
Failures in systems, processes or information technology (IT) infrastructure	Failures in IT systems, processes or infrastructure

Level 1	Level 2
Failure to execute, meet deadlines or manage the institution's activities	Transaction collection, execution and maintenance
	Monitoring and reporting
	Client acquisition and documentation
	Management of current accounts and non-account holders
	Other parties in Transactions
	Representatives and suppliers