## Index:

## 01. OBJECTIVE

This policy forms part of the continuous and integrated risk management framework of the BOCOM BBM Financial Conglomerate ("BOCOM BBM") and aims to establish a set of principles and guidelines to support the strategy for the control and management of **Operational Risk** at BOCOM BBM.

## 02. CONCEPTUAL FRAMEWORK/DEFINITIONS

### 02.01. **Operational Risk**

As established in Article 32 of Resolution No. 4,557 (2017), Operational Risk is defined as the possibility of direct or indirect loss resulting from external events or from deficiencies, inadequacies or failures in internal processes, people or systems.

The definition also encompasses legal risk, associated with inadequacies or deficiencies in contracts entered into by the institution, sanctions resulting from non-compliance with legal provisions, and compensation for damages to third parties arising from the institution's activities.

### 02.02. **Operational Risk Categories**

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

#### 02.02.01. Internal Fraud

Losses resulting from acts intended to defraud, misappropriate assets, or circumvent regulations, laws or company policies, involving at least one internal party.

#### 02.02.02. External Fraud

Losses resulting from acts intended to defraud or misappropriate assets committed by third parties, including money laundering, identity theft and misrepresentation of assets or revenues.

#### 02.02.03. Employment Practices and Inadequate Workplace Safety

Losses arising from inadequate or ineffective recruitment of personnel, lack of talent management, insufficient training and/or high turnover. It also includes losses resulting from acts inconsistent with employment contracts or labour laws, health and safety matters, compensation claims for personal injury, or diversity/discrimination-related events.

#### 02.02.04. Improper practices related to end users, clients, products and services

Losses resulting from an unintentional or negligent failure to fulfil a professional obligation towards specific clients (including fiduciary duties and suitability requirements), or from the nature or design of a product or service. These may include missed project deadlines or budgets, as well as missed, incomplete and/or low-quality deliverables.

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

Losses resulting from damage to physical assets (facilities) caused by natural disasters or other events (including human action).

#### 02.02.06. Events Leading to interruption of activities (unavailability) or discontinuity of services

Losses resulting from disruption of business activities caused by the absence or failure in the provision of essential services, whether from internal or external parties.

#### 02.02.07. Failures in systems, processes or IT infrastructure

Losses resulting from failures in systems, processes or IT infrastructure due to internal factors (e.g. backup failure, system unavailability) or external factors (e.g. poor performance of service providers, natural events).

#### 02.02.08. Failures in execution, deadline compliance and activity management (process failures)

Losses resulting from deficiencies in the administration, execution and management of activities associated with the institution's business processes.

#### 02.02.09. Information Security Breach

Losses resulting from theft, unauthorised access or leakage of personal or sensitive data. This includes losses associated with unauthorised access to systems due to lack of segregation, hacking, or system damage, among other causes.

### 02.03. **Risk factors**

- People: related to competence, ethical conduct and performance of duties;
- Processes: workflows and stages in product/service development and organisational activities, internal regulations and compliance with legislation;
- Technological: systems, infrastructure and IT architecture, storage and processing capacity and networks;
- External: related to environmental conditions, regulatory environment and social environment (including third parties such as service providers).

### 02.04. **Operational Loss**

In accordance with §1 of Article 34 of Resolution No. 4,557 of 2017, operational loss is defined as the quantifiable amount associated with operational risk events described in items 02.01 and 02.02. Operational losses associated with credit risk, market risk, social risk, environmental risk and climate risk must be included in the operational risk database, irrespective of whether they are also recorded in other databases.

In accordance with the definition established in Article 3 of BCB Circular No. 3,979 of 30 January 2020, and the amendments introduced by BCB Resolution No. 556 of 1 April 2026, operational losses must be

recorded and measured consistently with the institution's accounting records, observing the following concepts:

I. Gross loss amount: the quantifiable amount associated with the operational risk event, including provisions and expenses, prior to any recovery;

II. Recovered amount: financial resources effectively received from third parties for the purpose of reimbursing or indemnifying the institution for an operational loss, provided that such amounts are duly evidenced and recorded in the accounting records;

III. Net loss: corresponds to the effective loss amount net of recovered amounts, including provisions for contingencies and their respective reversals.

Amounts arising from related parties, amounts not recognised as accounting income, or positive effects resulting from tax deductibility shall not be considered as recoveries.

#### 02.04.01. Effective loss

An effective loss arises from the occurrence of an operational risk event that caused financial or accounting loss to the institution, directly impacting its results.

#### 02.04.02. Non-Effective or Potential Loss

A situation in which operational risk events did not result in an effective loss to the institution due to the intervention of an internal or external party prior to the materialisation of the loss.

### 02.05. **Operational Incident**

An occurrence of non-compliance events associated with operational risks (as defined in items 02.01 and 02.02), originating from one or more risk factors (as defined in item 02.03), which may or may not result in operational losses (as defined in item 02.04).

### 02.06. **Significant Operational Incident**

An operational incident that:

- Has resulted or could result in significant financial losses;
- Has affected or could significantly affect business processes;
- Has caused or could cause damage to data or sensitive information, or otherwise have a significant impact on clients or on the Institution's reputation.

Criteria providing guidance on the assessment of the relevance of an operational incident are disclosed on the Internal Controls department intranet.

### 02.07. **Cyber Risk**

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

### 02.08. Cyber Incidents

An event related to the cyber environment that: a) produces an adverse effect or represents a threat to information technology (IT) systems or to the information that such systems process, store or transmit; or b) breaches security policies or procedures related to IT systems.

### 02.09. Significant Cybersecurity Incident

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

### 02.010. Business Continuity Management

Consists of a set of strategies aimed at ensuring the continuity of the institution's activities and limiting losses resulting from the interruption of critical business processes. The Business Continuity Management framework comprises:

- The Business Continuity Policy, aimed at establishing the organisational structure and the main guidelines and rules;
- Business Continuity Plans, which establish procedures and estimated timeframes for the resumption and recovery of activities in the event of interruption of critical business processes, as well as the necessary communication actions;
- Business Impact Analysis (BIA), whose purpose is to identify the main critical processes and supporting assets, determine the key factors for the implementation of contingency plans, and ensure that critical systems are restored as a priority in the event of disruption;
- Análise de Impacto nos Negócios (BIA - *Business Impact Analysis*), cujo objetivo é identificar os principais processos críticos e ativos que o suportam, determinar os principais fatores para implementação de planos de emergências e garantir que os principais sistemas sejam restaurados primeiro no caso de uma interrupção.
- Testing and periodic review of business continuity plans, at an appropriate frequency.

## 03. SCOPE / INVOLVED AREAS

### 03.01. Scope of the Risk Management Framework

The risk management framework shall be:

- Compatible with the business model, the nature of operations, and the complexity of BOCOM BBM's current products, services, activities and processes;
- Proportionate to the size and relevance of risk exposure, in accordance with the criteria defined by the institution in the Risk Appetite Statement (RAS);
- Appropriate to the risk profile and to the systemic importance of BOCOM BBM; and
- Capable of assessing risks arising from macroeconomic conditions and from the markets in which BOCOM BBM operates.

In addition, it shall be aligned with the classification segment, in accordance with Article 2 of Central Bank Resolution No. 4,553 of 2017, under which the Bank is currently classified. The information described herein is aligned with Segment 3 (S3). Should BOCOM BBM be reclassified into Segment 1 (S1) or Segment 2 (S2), this document shall be reviewed accordingly.

The operational risk management framework of BOCOM BBM shall provide for:

- Policies establishing decision-making criteria for the outsourcing of services and for the selection of service providers, including the minimum contractual conditions required to mitigate operational risk;
- Implementation of an IT governance framework consistent with the risk appetite levels defined in the RAS;
- IT systems, processes and infrastructure that:
    a) ensure the integrity, security and availability of data stored, processed or transmitted, as well as of the information systems used;
    b) include protection and security mechanisms for networks, websites, servers and communication channels in order to reduce vulnerability to cyber-attacks;
    c) adopt procedures to monitor, track and restrict access to sensitive data, networks, systems, databases and security modules;
    d) monitor data security breaches and complaints from end users in this regard; and
    e) are appropriate to the needs of, and changes in, the business model, both under normal conditions and during periods of stress.

### 03.02. Scope of the Policy

This policy applies to the BOCOM BBM Conglomerate and its STAKEHOLDERS. STAKEHOLDERS include employees, interns, shareholders, clients, counterparties, suppliers, and the communities in which we operate.

### 03.03. Organisational Structure

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

In addition, the Compliance and Internal Audit functions, acting independently, autonomously and impartially, are responsible for assessing the quality and effectiveness of the institution's internal control systems and processes, risk management framework, and corporate governance within BOCOM BBM.

## 04. RESPONSABILITIES

### 04.01. Responsible for the execution of the duties set forth in this policy

With regard to execution, the units below have the following responsibilities:

#### 04.01.01. Board / Risk Committee / Executive Management

- To approve annually the operational risk management policy for BOCOM BBM institutions;
- To define the operational risk appetite levels of BOCOM BBM in the RAS; and
- To take strategic decisions for the control of Operational Risk.

#### 04.01.02. Operational Risk and Internal Controls Committee

- To promote a culture oriented towards risk management;
- To define roles and responsibilities of each member of the Operational Risk structure;
- To inform the Risk Committee regarding compliance with its recommendations and enquiries concerning the proper functioning of the operational risk management system;
- To analyse significant operational incidents that have occurred and, where necessary, decide on actions to be taken in order to mitigate the risks incurred;
- To assess the operational risk appetite levels defined in the RAS and the strategies for their management;
- To analyse significant situations of exposure of the institution to operational risks, proposing the necessary adjustments to the organisation; and
- To analyse situations not covered by this policy.

#### 04.01.03. Internal Controls

- To propose an operational risk management policy and suggest amendments, when necessary, for approval by the Board of Directors and Executive Management;
- To promote awareness of operational risk in order to ensure that all employees are fully aware of the importance of operational risk management.

With regard to macro-processes and processes:

- To identify, together with the business areas, each macro-process/process existing within BOCOM BBM;
- To seek to develop, jointly with area managers, procedures describing the (macro)processes, including the identification of inherent operational risks and respective controls;
- To seek to establish, jointly with area managers, key risk indicators; and
- To assess the potential effects of the operational risks to which BOCOM BBM is exposed and report its conclusions internally and externally, where necessary.

Assessments are prioritised and frequently carried out when:

a. A significant operational incident has occurred in the Bank or in other banks;
b. Exposure of the Bank to a significant operational risk has been identified;
c. There are significant changes in procedures of any operation;
d. There are significant changes in operational systems;
e. New products are launched;

f. Regulation with significant impact is issued or updated;
g. At the request of the regulator or of Executive Management.

With regard to operational risk events:

- To manage the operational risk event database;
- To periodically monitor identified operational risks in order to verify whether the mitigating actions adopted are effective and/or whether there is an increase in the frequency of incidents related to such risks;
- To prepare assessment reports on significant operational incidents, identifying the controls established to remediate identified failures and any operational losses.

With regard to outsourced processes:

- To identify risks and controls in processes for which services are outsourced;
- To keep the Supplier Selection, Contracting and Management Policy updated with regard to the criteria for outsourcing decisions and the selection of service providers, including the minimum contractual conditions required to mitigate operational risk.

With regard to business continuity:

- To ensure business continuity management, including the strategies to be adopted to secure contingency conditions for the most critical activities and to mitigate severe losses arising from operational risk.

With regard to regulatory reporting:

- In conjunction with the Compliance area, to submit reports to the governing bodies and make them available to the CVM by the last business day of April each year, containing operational risk events, their risk assessment, and the progress/conclusion of any mitigating actions;
- In conjunction with the Compliance area, to communicate Significant Cybersecurity Incidents, in accordance with the deadlines and recipients defined in applicable regulations and internal policies. Such incidents must be reported to BSM on a monthly basis;  as vigentes e nas políticas internas. Os incidentes devem ser comunicados à BSM mensalmente.
- To submit to the Central Bank of Brazil the Operational Risk Statement (DRO), document code 5050, on a semi-annual basis, as of 30 June and 31 December, containing the information from the operational risk database, in accordance with BCB Circular No. 3,979 of 30 January 2020 and BCB Normative Instruction No. 700 of 13 January 2026. For BOCOM BBM, classified under Segment 3 (S3), submission shall be required as of the 2026 reference dates.

With regard to the limits established in the RAS:

- To be responsible for calculating, assessing and reporting, and where necessary ensuring the re-alignment of, the operational risk indicators and the information technology indicators set out in the

RAS. The description, calculation and monitoring of such indicators are set out in the Risk Appetite Management procedure.

#### 04.01.04. Information Technology (IT)

- To provide the necessary technological support for the development of operational risk monitoring and control activities.

#### 04.01.05. Information Security

- To assist, in coordination with the Internal Controls area, in the integrated identification of risks to the Institution;
- To analyse cyber risk incidents and inform the Risk Committee of any mitigating actions or impacts on the Institution's processes;
- To review security and data confidentiality measures, especially after the occurrence of failures and prior to changes in infrastructure or procedures;
- To perform tests to ensure the robustness and effectiveness of the data security measures adopted;
- To prepare reports indicating procedures to remediate identified failures.

#### 04.01.06. Internal Audit

- To periodically assess the quality, integrity, consistency and governance of the operational risk database, including the processes of identification, collection, processing, aggregation and reporting of information;
- To verify the adherence of operational risk management processes and the database to applicable regulations, as well as to the institution's internal policies;
- To carry out prior assessment of requests for deletion of events from the operational risk database, issuing an opinion on their adequacy, justification and the absence of residual exposure associated with the events proposed for removal;
- To report any identified deficiencies and monitor the implementation of corrective action plans.

#### 04.01.07. Process Owners Managers

- To maintain awareness of the risks inherent to their processes, assessing their likelihood of occurrence and potential impacts;
- To assist in the preparation of process mappings;
- To inform about changes in processes, routines and controls that may affect the assessment of risk exposure;
- To manage business activities in accordance with senior management guidelines, including the definition of Risk Appetite; and
- To promote awareness of operational risk to ensure that all employees fully understand the importance of operational risk management.

#### 04.01.08. **Other employees of the institution**

All employees are responsible, when identifying occurrences related to operational risks, for immediately communicating them to the Internal Controls area so that the appropriate measures may be taken.

### 04.02. **for Monitoring the Execution of the Duties Set Forth in this Policy**

The Manager of the Internal Controls area is responsible for monitoring the execution of the duties set forth in this policy.

### 04.03. **Responsible for the maintenance of this policy**

The Internal Controls area is responsible for the maintenance of this policy.

## 05. APPROVAL LEVELS

The Operational Risk and Internal Controls Committee, Executive Management and the Board of Directors shall approve this policy.

The Operational Risk and Internal Controls Committee shall analyse situations not covered by this policy and assess whether approval by the Board of Directors is required.

## 06. GUIDELINES:

### 06.01. **Principles**

#### 06.01.01. Best Practices

The Internal Controls area, responsible for operational risk management, analyses and monitors the best control practices to be adopted in order to ensure the security and reliability of processes.

#### 06.01.02. Integrated Risk Management

Upon identification of an operational risk, the Internal Controls area shall seek to analyse its potential impact on other risks managed by the Bank. Currently, the main risks that BOCOM BBM seeks to measure, assess, monitor, report, control and mitigate are:

- credit risk;
- market risk;
- liquidity risk;
- strategic risk;
- regulatory risk;
- reputational risk;
- information security risk;
- social risk;
- environmental risk;
- climate risk; and

- operational risk, as addressed in this policy.

Risk management shall be integrated, enabling the identification, measurement, assessment, monitoring, reporting, control and mitigation of adverse effects resulting from the interaction between the risks mentioned above.

#### 06.01.03. Information Transparency

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

#### 06.01.04. Risk-Oriented Culture

The operational risk management culture is disseminated across all areas of the institution as well as to its related parties. Whenever possible, training sessions shall be conducted in order to reinforce the importance of operational risk management.

### 06.02. **Phases of Operational Risk Management**

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

#### 06.02.01. Preventive Phase

##### Objective

The objective of this phase is to identify operational risk events prior to their materialisation and to develop methods that enable the risk to be avoided, mitigated, transferred or accepted.

##### Stages

It shall comprise the following stages:

I. Identification: to identify operational risk events, indicating areas of occurrence, causes and potential financial impacts.
II. Assessment: to quantify exposure to operational risk in order to assess its impact on the business.
III. Control: to record the behaviour of operational risks, limits, indicators and operational loss events, as well as to implement mechanisms to ensure that operational risk limits and indicators remain within defined levels.
IV. Mitigation: to develop and implement mechanisms to mitigate operational risk, aiming to reduce losses.
V. Monitoring: to identify deficiencies in the operational risk management process.

##### Tools

Examples of tools that support the mitigation of operational risks during the preventive phase include:

- 
- Definition of Policies and Codes of Ethics and Conduct;

- Process Mapping and development of Flowcharts;
- Formalisation of Operational Manuals;
- Training;
- Establishment of Monitoring activities;
- Implementation of access controls (physical and logical), installation of antivirus software, and periodic data backup;
- Business Continuity Testing; among others.

#### 06.02.02. Reactive Phase

##### Objective

The objective of this phase is to address operational risk events that have already materialised, which may or may not have resulted in operational losses.

##### General Stages

I. Receipt of the incident occurrence record;
II. Analysis of its causes and of the impacts on business processes;
III. Identification of the event in relation to other types of risk (e.g. cyber risk or social and environmental risk);
IV. Guidance regarding the actions to be taken for short-term resolution and to prevent the occurrence of new incidents

### 06.03. **Incident Recording**

#### 06.03.01. Who may record an incident?

Once an incident has occurred, any employee may report it. The record shall be made via an electronic form, available on all employees' browsers, and shall be subject to assessment/approval by the manager of the reported area, risk classification by the manager of the impacted area, and classification of the likelihood of occurrence by the manager of the originating area.

It should be noted that the Internal Controls area may also classify the likelihood of occurrence, taking into account historical information available in the incident database.

#### 06.03.02. Incident Database

For each incident record, the following information shall be stored:

- The internal identification code of the operational risk event;
- The operational risk category, as per item 02.02;
- The risk factors, as per item 02.03, indicating the name of the process, system or the relevant external factor;
- The identification of the business unit where the occurrence took place, as per Annex I, item 014.01 of this policy;

- The dates of occurrence and detection;
- A description of the event, including, where possible, the root cause;
- The short-term solution;
- The mitigating controls implemented to prevent the recurrence of the event;
- The impacted areas;
- The impacted processes;
- The accumulated gross loss amount (where applicable);
- The accumulated loss amount recovered through insurance or other means (where applicable);
- The source of reimbursement, for loss recovery events (where applicable);
- The classification, based on consistent and verifiable criteria, of Level 1 Category and Level 2 Category to which the operational risk event belongs, as per Annex II of this policy;
- The association, where applicable, with other types of risk to which the Bank is exposed: credit risk, market risk, social and environmental risk, liquidity risk, regulatory risk, reputational risk, and cyber risk.

### 06.03.03. Loss treatment

For the purpose of building the internal loss database, operational risk losses materialised in the form of expenses shall be considered.

The recording and treatment of operational losses shall follow the concepts of gross loss amount, recovered amount and net loss defined in section 02.04 of this policy, ensuring consistency with the institution's accounting records and applicable regulatory requirements.

### 06.03.04. Aggregation of operational risk events

Operational risk events shall be recorded on an individual basis, and aggregation shall only be permitted when they share the same root cause, based on consistent, traceable and verifiable criteria.

Event aggregation shall observe:

I. the existence of a common causal link between the events;
II. consistency in risk classification;
III. maintenance of documentation supporting the criteria used for aggregation.

Aggregation of events that do not have a direct relationship with each other is not permitted.

Where applicable, an identifier shall be maintained to allow linkage between individual events and the aggregated event, ensuring traceability of information and transparency of the database.

The adoption of aggregation criteria shall not compromise the quality of the information used for risk monitoring, regulatory reporting or capital calculation purposes.

#### 06.03.05. Request for additional information

Following registration in the Internal Controls database, incidents shall be analysed and their root causes identified.

It should be noted that, in addition to Internal Controls, the Risk, Information Security and Internal Audit areas, as well as the Operational Risk and Internal Controls Committee, are also notified of incident records. Each of these functions may request additional information, if deemed necessary, either from those involved in the event or from the employee who submitted the report.

### 06.04. **Fraud Reporting**

BOCOM BBM adopts a zero-tolerance approach towards any form of fraudulent activity by its employees, service providers, agents or brokers. Fraudulent activity is understood to include forgery, misappropriation of funds, theft, personal use of assets, active and passive corruption, embezzlement, questionable payments and receipts, administrative misconduct, among others.

With the objective of consistently delivering reliable results with full transparency and security, all fraud cases shall be reported to the Compliance Department so that appropriate investigations may be initiated. Due to their sensitive nature, suspected fraud cases shall be handled confidentially.

### 06.05. **Significant security incidents**

Upon identification of an incident involving damage to information integrity, data leakage or cyber-attacks, the Internal Controls area shall notify the Information Security area. This area is responsible for escalating such events to the Information Security Committee and for monitoring any established remediation actions.

The Information Security area is responsible for reaffirming the institution's commitment to the confidentiality, authenticity, integrity and availability of data and sensitive information, as well as adopting measures to reduce exposure to cyber-attacks.

Security incidents considered significant shall be reported to the Central Bank and to the Superintendence of Market and Intermediary Relations (SMI).

### 06.06. **Incidents triggering the Business Continuity Plan**

Any event that results in the activation of the business continuity plan shall be reported to the governing bodies and to the SMI.

Such reporting shall include the causes of the activation, indicating the affected critical processes. Additionally, it shall include the mitigating actions adopted or planned, the time taken to resolve the event, and any other relevant information.

## 07. FINAL CONSIDERATIONS

This document is for strictly internal use and shall not be made available to third parties without prior consultation with the Head of the Internal Controls area.

## 08. RELATED LEGISLATION / REGULATION

- Operational Qualification Programme (PQO) Guidelines, dated 02 January 2025;
- CMN Resolution No. 5,076, dated 18 May 2023;
- CMN Resolution No. 4,557, dated 23 February 2017;
- BCB Circular No. 3,979, dated 30 January 2020;
- BCB Normative Instruction No. 33, dated 29 October 2020;
- BCB Resolution No. 356, dated 28 November 2023;
- CMN Resolution No. 4,893, dated 26 February 2021;
- CVM Resolution No. 35, dated 26 May 2021;
- CMN Resolution No. 4,943, dated 15 September 2021;
- CMN Resolution No. 4,968, dated 25 November 2021;
- BCB Normative Instruction No. 700, dated 13 January 2026;
- BCB Resolution No. 556, dated 1 April 2026.

## 09. INTERNAL REFERENCES

- Risk Appetite Statement;
- Internal Controls Policy;
- Market Risk Management Policy;
- Credit Risk Management Policy;
- Liquidity Risk Management Policy;
- Business Continuity Management Policy;
- Capital Management Policy;
- Information Disclosure Policy;
- Data Protection Policy;
- Information Security Policy;
- Backup and Restore Policy;
- Product Approval Policy; and
- Process Assessment 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. | 2007-06-27 | Document Creation | Operational Risk |
| 2. | 2008-12-10 | Document Revision | Operational Risk |
| 3. | 2009-12-14 | Document Revision | Operational Risk |
| 4. | 2010-12-31 | Document Revision | Operational Risk |
| 5. | 2011-12-13 | Document Revision | Operational Risk |
| 6. | 2012-12-03 | Document Revision | Operational Risk |
| 7. | 2013-12-04 | Document Revision | Operational Risk |
| 8. | 2014-12-13 | Document Revision | Operational Risk |
| 9. | 2015-12-29 | Document Revision | Operational Risk |
| 10. | 2016-12-30 | Document Revision | Operational Risk and Internal Controls |
| 11. | 2017-12-26 | Document Revision | Operational Risk and Internal Controls |
| 12. | 2018-03-27 | Document Revision | Operational Risk and Internal Controls |
| 13 | 2018-12-31 | Document Revision | Operational Risk and Internal Controls |
| 14 | 2019-12-31 | Document Revision | Operational Risk and Internal Controls |
| 15 | 2021-01-31 | Document Revision | Operational Risk and Internal Controls |
| 16 | 2022-01-31 | Document Revision | Operational Risk and Internal Controls |
| 17. | 2023-01-31 | Document Revision | Operational Risk and Internal Controls |
| 18. | 2023-08-02 | Document Revision | Operational Risk and Internal Controls |
| 19. | 2024-01-02 | Document Revision | Operational Risk and Internal Controls |
| 20. | 2025-01-02 | Document Revision | Operational Risk and Internal Controls |
| 21. | 2025-06-09 | Document Revision | Operational Risk and Internal Controls |
| 22. | 2026-06-12 | Document Revision | Operational Risk and Internal Controls |

## 013. APPROVALS

_____

Tatiana Ferro – Operational Risk and Internal Controls General Manager

_____

Monique Verboneen – CRO (Chief Risk Officer)

## 014. ANNEXES

### 014.01. **Business Units**

| |
|---|
| Corporate Finance |
| Trading and Sales |
| Retail |
| Commercial |
| Payments and Settlements |
| Financial Agent Services |
| Asset Management |
| Retail Brokerage |

### 014.02. Operational Risk Categories

| Level 1 | Level 2 |
|---|---|
| Internal Fraud | Theft and Fraud (internal origin) |
| | Unauthorised Activity |

| Level 1 | Level 2 |
|---|---|
| External Fraud | Theft and Fraud (external origin) |
| | Systems Security |
| | Other types of external Fraud |

| Level 1 | Level 2 |
|---|---|
| Employment practices and inadequate workplace safety | Employment relations |
| | Diversity and discrimination |
| | Workplace safety |

| Level 1 | Level 2 |
|---|---|
| Improper practices related to clients, products and services | Client suitability, disclosure of information on products and services, breach of fiduciary duty |
| | Improper business and market practices |
| | Product defects |
| | Selection, sponsorship and exposure |
| | Advisory activities |

| Level 1 | Level 2 |
|---|---|
| Damage to physical assets owned by or in use by the institution | Disasters and other events |

| Level 1 | Level 2 |
|---|---|
| Events leading to business disruption | Business disruption |

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

| Level 1 | Level 2 |
|---|---|
| Execution, delivery and process management failures | Transaction capture, execution and maintenance |
| | Monitoring and reporting |
| | Client onboarding and documentation |
| | Account management (Clients and Non-Clients) |
| | Counterparties in transactions |
| | Representatives and Suppliers |