OPERATIONAL RISK POLICY

1. OBJECTIVE

The operational risk policy, hereinafter referred to as POLICY, establishes the operational risk management framework, through guidelines, roles and responsibilities adopted for managing operational risk, under the terms of Resolution 4,557, of February 23, 2017, published by the National Monetary Council (CMN).

2. GUIDELINES

2.1. Scope

The following are subject to the POLICY:

I. All companies of the Prudential Conglomerate and their subsidiaries, according to the corporate structure in effect, hereinafter referred to as SAFRA;
II. All employees, regardless of their jobs or duties; and
III. All companies that provide outsourced services material to the operation of the institution and their employees.

2.2. Definitions

Operational Risk

Operational risk is the possibility of incurring losses resulting from external events or failure, deficiency or inadequacy of internal processes, people or systems.

Operational risk also includes the legal risk associated with the inadequacy or deficiency in contracts signed by SAFRA, as well as sanctions in view of the breach of legal provisions, and damages to third parties arising from the activities performed by SAFRA. The assessment of legal risk is performed on ongoing basis in the legal areas of SAFRA and specific Committees.

This definition excludes Reputational/Image and Strategic/Business risks.

Operating Loss

Operating loss is the quantifiable amount associated with operational risk events.

Among the operational risk events, the following are included:

I. Internal frauds;
II. External frauds;
III. Labor claims and deficient occupational safety;
IV. Inappropriate practices related to customers, products and services;
V. Damages to own physical assets or assets in use by the institution;
VI. Situations that cause disruption to the institution's activities;
VII. Failures in Information Technology (IT) systems, processes or infrastructure;
VIII. Failures in the execution, timing and management of the institution's activities.

The event of social and environmental loss was included in the base of operating losses in a specific category (IX – Social and Environmental Loss).

2.3. Operational Risk Management Framework

The Operational Risk area is an independent control unit (UC), segregated from the unit that executes the internal audit activity, and is responsible for identifying and monitoring operational risks, and evaluating the need for control and mitigation, as well as for the formulation, dissemination, and maintenance of this POLICY.

SAFRA adopts the strategy of three lines of defense as primary means to operationalize its Operational Risk management framework, including Internal Controls, and assure that the guidelines set out by adopting an integrated approach are followed. The three lines of defense are as follows:

- First line of defense: it is the operational or business area, ratifying the alignment of SAFRA's business strategies with the risk management ones. It is responsible for managing and responding to risks, monitoring and implementing operational risk

mitigation actions and self-assessment, according to the methodology established by the Internal Control area;

- Second line of defense: the Internal Control and Compliance areas represent the second line of defense, being responsible for establishing the Self-assessment and Independent Assessment methodologies, supporting business areas in the process of identification, measurement, assessment, mitigation (through controls), monitoring and reporting of operational risks, and guaranteeing SAFRA's regulatory compliance; and
- Third line of defense: Internal Audit, as third line of defense, is responsible for the ongoing independent assessment of risk management-related processes.

Aimed at assuring the fulfillment of the regulatory and internal policies by all collaborators of Safra Prudential Conglomerate, Senior Management established that the programs comprising the management of results and performance also consider the indicators related to the breach of policies. The responsibility for adopting this guideline rests with managers, with centralization in the Planning and Control Advisory area.

The Operational Risk management framework, hereinafter referred to as FRAMEWORK, is described in public report, at least annually, and is comprised as follows:

Board of Directors:

I. Approve and revise, upon the Superior Risk Committee's recommendations:
   a. The operational risk management policies, strategies and limits;
   b. The operational risk capital management policies and strategies;
   c. The operational risk stress testing program;
   d. The policies on going concern management;
   e. The capital plan for operational risk;
   f. The capital contingency plan for operational risk.

II. Set SAFRA's operational risk appetite levels in the RAS[1] and revise them, through the Superior Risk Committee and CGROC;

III. Assure SAFRA's adherence to the operational risk management policies, strategies and limits;

IV. Assure that SAFRA maintains appropriate and sufficient capital levels for operational risk;

V. Assure the timely correction of the deficiencies in the risk and capital management framework for operational risk;

VI. Authorize, when necessary, the exceptions to the policies, procedures, limits and occasional extrapolations, and to the operational risk appetite levels set in the RAS, through the Superior Risk Committee and CGROC;

VII. Assure appropriate and sufficient funds to perform activities of operational risk management and capital management for operational risk, in an independent, objective and effective way;

VIII. Assure that the compensation structure adopted by SAFRA does not encourage behaviors incompatible with the risk appetite levels set in the RAS;

IX. Promote the dissemination of the operational risk management culture in SAFRA.

Superior Risk Committee:

I. Propose, at least annually, recommendations to the Board of Directors about the following:
   a. The operational risk management policies, strategies and limits;
   b. The operational risk capital management policies and strategies;
   c. The operational risk stress testing program;
   d. The policies on going concern management;
   e. The capital plan for operational risk;
   f. The capital contingency plan for operational risk.

II. Evaluate the operational risk appetite levels set in the RAS and the strategies for managing them;

III. Evaluate the adherence level of the operational risk management framework's process to the Policy;

IV. Assure the existence of a specific unit that acts independently and is responsible for the operational risk management in the organizational structure, compatible with the institution's business model, nature of operations, complexity of products, services, activities and processes, as well as proportional to the size and relevance of the

[1] RAS: Risk Appetite Statement

exposure to risks, appropriate to SAFRA's risk profile and systemic importance, and able to evaluate its risks.

Operational Risk and Compliance Risk Management Committee (CGROC):

I. Carry out its responsibility as a forum that drives and make decisions on the issues related to the operational risk management in SAFRA;
II. Address the operational risk as a separate risk category to be managed, in its deliberations;
III. Supervise the activities and evaluate the works of the Operational Risk area related to operational risk management;
IV. Deliberate about points of divergence not resolved in the Regular Internal Controls Committee (CCI Regular);
V. Deliberate about methodologies for capital allocation for operational risk, and quantification and monitoring of Operational Risk Appetite;
VI. Submit to the Superior Risk Committee (GIR) significant changes and/or exceptions, in SAFRA's policies and strategies, as well as in its systems, routines, and procedures, besides occasional extrapolations of the operational risk appetite levels set in the RAS.

Chief Risk Officer (CRO):

I. Supervise the development, implementation and performance of the operational risk management framework, including its improvement;
II. Address the operational risk as a separate risk category to be managed, in its deliberations;
III. Guarantee the appropriate capacity building of the members of the operational risk management framework about risk management policies, processes, reports, systems, and models, even if developed by third parties;
IV. Support and participate in the strategic decision-making process related to the operational risk and capital management, assisting the Board of Directors.

Operational Risk Area:

I. Implementation of the operational risk management framework;
II. Preparation and dissemination of Rules and Policies on operational risks management and capital management for Operational Risk;
III. Risk identification – determine the origin of risks and weaknesses in the processes of SAFRA and material outsourced services
IV. Risk assessment and measurement - proposition about Key Risk Indicators (ICR), quantification of expected and unexpected losses, and calculation of the capital to be allocated for operational risk;
V. Risk mitigation – development of control mechanisms and action plans for mitigation of identified operational risks and preparation of going concern plans;
VI. Risk control - follow-up of mitigation actions; proposition, implementation and follow-up of control actions; determination of the compliance level of processes; and backtesting;
VII. Risk monitoring - monitoring of operating loss events, behavior of Key Risk Indicators (ICR), exposure limits, as well as the existence of internal controls and going concern plans, and risks arising from outsourcing of critical services;
VIII. Management of the information on losses related to operational risk – loss base;,
IX. Coordination of operating loss management committees, identification of the root causes and action plans for correction/mitigation;
X. Development of models and methodologies for quantifying economic capital for Operational Risk;
XI. Preparation and adoption of the methodology for calculating stress, in compliance with Circular 3,846/17, as well as Section II of CMN Resolution 4,557/17;
XII. Backtesting of the implemented operational risk control models and systems;
XIII. Preparation of short- and long-term capital projections together with the Finance Area;
XIV. Preparation of the annual report on the ICAAP for Operational Risk and Operational Risk Report;
XV. Indicate among the outsourced service providers those that have the highest materiality to the operations of SAFRA;
XVI. Follow-up of the contingency plan containing the strategies to be adopted for assuring conditions for the going concern of activities and limit severe losses arising from operational risk;
XVII. Training and dissemination of the Operational Risk management culture;
XVIII. Support to product and service management áreas.

Information Security:

I. Preparation of the Policy on Going Concern Management;
II. Assist the business areas in the development, maintenance, and creation of going concern plans, coordinating tests in the going concern area (ACN), attesting the availability of the Matrix environment in case of any operational disruptions.

Operational Risk and Internal Control Officer:
Each operational or business area has an Operational Risk and Internal Control Officer, with at least Executive Superintendent position, or, in the absence of such position, for the collaborator with position immediately below, which represents the first line of defense, with the following attribution:

I. Assure that the risks of the activities under her/his management are duly identified, controlled, monitored and mitigated;
II. Establish risk mitigation procedures, disclosing them to all involved in the processes;
III. Assure the adoption of operational risk management methodologies;
IV. Prepare the risk and control matrix, keeping it updated;
V. Run tests to assure the effectiveness of risk mitigation controls and report their results to the Operational Risk area;
VI. Assure the reporting of all identified control events and failures to the Operational Risk area;
VII. Document and keep updated the documentation of Policies, Rules, Procedures and other documents of her/his area;
VIII. Disseminate the risk and control culture in the area(s) under her/his responsibility; assuring the compliance with internal rules and regulatory aspects, with zeal for the effectiveness and integrity of controls;
IX. Timely follow-up and inform about the frauds or suspected frauds to the hierarchy and/or Internal Audit, for taking the necessary measures, maintaining the appropriate secrecy.

Operational or Business Areas:
They represent the first line of defense in operational risk management, with the following attributions:

I. Application of operational risk management methodologies;
II. Identification, documentation, record, and reporting to the Operational Risk area of all operating losses resulting from failure, deficiency, or inadequacy of internal processes, persons, systems, or external events;
III. Business management following the guidelines from senior management, such as the setting of Risk Appetite;
IV. Information on all identified control events and failures to the Operational Risk area;
V. Evaluation of the exposure to the operational risk arising from the engagement of the material outsourced service providers, for the regular operation of the institution or in situations of contingency;
VI. Notification to the Operational Risk area of any and all material exposure to operational risk.

Finance Area:

I. Capital Management and consolidation of the ICAAP report;
II. Coordination of the capital plan and capital contingency plan preparation;
III. Coordination of stress test events;
IV. Preparation of short- and long-term capital projections together with the risk management areas;
V. Provision of accounting and managerial information to the risk control and management areas;
VI. Monitoring of the adequacy of capital maintained in face of the capital need estimate;
VII. Disclosure of the information required by BACEN related to the ICAAP;
VIII. Evaluation of the need for issuing equity instruments and/or changing capital composition;
IX. Proposition about actions for optimizing required capital and capital structure;
X. Provision of Regulatory Capital;

XI. Performance of independent validations of Operational Risk for ICAAP, preparation of the report on independent technical validation of models and methodologies comprising the annual ICAAP report;

XII. Application of the capital allocation model and procedures for calculating the portion of Risk-weighted Assets (RWA), related to the calculation of the capital required by BACEN for operational risk through the standardized approach (RWAopad – ASA 2).

Validity: Exercise of 2018 **Review:** April of 2019