Safra

Tradição Secular de Segurança

Operational Risk Policy

1. OBJECTIVE

The operational risk policy, referred to in this document as POLICY, establishes the structure of operational risk management, through guidelines, roles and responsibilities adopted for operational risk management, in accordance with Resolution nº 4557, of February 23, 2017, Published by the Brazilian Monetary Council (English translation for Conselho Monetário Nacional - CMN).

2. GUIDELINES

2.1. Coverage

Are subject to the POLICY:

(i) All companies belonging to the Prudential Conglomerate and their subsidiaries, according to the current corporate structure, hereinafter referred to as SAFRA;

(ii) All employees, regardless of position or function;

(iii) All companies providing outsourced services relevant to the operation of the institution and its employees.

2.2. Definitions

Operational Risk

Operational Risk is defined as the possibility of losses resulting from external events or failure, deficiency or inadequacy of internal processes, people and systems.

The operational risk also includes the legal risk associated with the inadequacy or dificiency in contracts signed by SAFRA, as well as penalties for non-compliance with legal provisions and damages for third parties resulting from the activities executed by Safra. The legal risk assessment is carried out continuously in the legal departments of SAFRA and in the specific committees.

This definition excludes reputational or image and strategic or business risk.

Operational Loss

Operational loss is the quantifiable value associated to operational risk events.

Operational risk events include:

I - internal fraud;

II - external fraud;

III - labor demands and poor workplace safety;

IV - improper practices to customers, products and services;

V - damage to the own physical assets or in use by the institution;

VI - situations that lead to the interruption of the institution's activities;

VII - failures in systems, processes or information technology infrastructure (IT);

VIII - failures in execution, compliance with deadlines and management of activities in the institution.

The event of social and environmental loss was included in the operational losses database in a specific category (IX - Social-Environmental Loss).

2.3. Operational Risk Management Structure

The Operational Risk department is an independent control unit (CU), segregated from the unit executing the internal audit activity, and is responsible for identification and monitoring of operational risks and assessment of need for control and mitigation, as well as elaboration, dissemination and maintenance of this POLICY.

SAFRA's adopts the strategy of three defense lines as the primary means to operationalize its Operational Risk Management structure, including Internal Controls, and ensure compliance with the guidelines defined through an integrated approach. The three lines of defense are:

(i) First line of defense: is the business or operational departments, ratifying the alignment of SAFRA's business strategies with the risk management. It's responsible for managing and response to risks, monitoring and implementing self-assessment and actions to mitigate operational risk, according to the methodology defined by the Internal Controls department;

(ii) Second line of defense: The Internal Controls and Operational Risks departments are the second line of defense, responsible for defining the Self-Assessment and Independent Assessment methodologies, to support business units in identification, measurement, assessment, mitigation (via controls), monitoring and reporting of operational risks processes and by ensuring the regulatory adherence of SAFRA; and

(iii) Third line of defense: The Internal Audit, as the third line of defense, is responsible for the continuous independent evaluation of the processes related to risk management.

The Operational Risk management structure is referred in this document as STRUCTURE, described in a public report, with a minimum annual periodicity, and it is composed as follows:

Administrative Council:

(i) Approve and review, through recommendation of Superior Risks Committee:
   a. the policies, strategies and bound of operational risks management;
   b. the policies and strategies of operational risk and capital management;
   c. the stress tests program of operational risks;
   d. the policies for Business Continuity Management;
   e. the capital plan for operational risks;
   f. the capital contingency plan for operational risks.

(ii) Set the levels of SAFRA's operational risks appetite in RAS[1] and review them, through the Risks Superior Committee and CGROC;

(iii) Ensure SAFRA's adherence to policies, strategies and management of operational risks bounds;

(iv) Ensure that SAFRA maintains adequate and sufficient capital levels for operational risks;

(v) Ensure the timely correction of weaknesses in the risk management and capital structure for operational risk;

(vi) To authorize, when necessary, exceptions to the policies, procedures, limits and possible extrapolations and the levels of operational risk appetite established in RAS, through the the Risks Superior Committee and CGROC;

(vii) Ensure adequate and sufficient resources for the exercise of activities of operational risk management and capital management for operational risk, in an independent, objective and effectively;

(viii) Ensure that the remuneration structure adopted by SAFRA does not encourage behaviors that are incompatible with the risk appetite levels established in the RAS.

(ix) Promote the dissemination of the operational risk management culture in SAFRA.

---

[1] RAS: Risk Appetite Statement

Risks Superior Committee:

(i) Propose, at least annually, recommendations of the Board of Directors about:

a. the policies, strategies and bound of operational risks management;
b. the policies and strategies of operational risk and capital management;
c. the stress tests program of operational risks;
d. the policies for Business Continuity Management;
e. the capital plan for operational risks;
f. the capital contingency plan for operational risks.

(ii) Evaluate the levels of operational risks appetite established in RAS and strategies for your management;

(iii) Evaluate the degree of adherence of operational risks management structure processes to Policy;

(iv) Ensure the existence of specific unit with independent actuation and responsible for operational risks management in organization's structure. compatible with institution's business model, operations nature, products complexity, services, activities and processes, as well as proportional to the size and relevance of exposure to risks, appropriate to the risk profile and systemic importance of SAFRA and able to evaluate its risks.

Operational Risk Management and Compliance Committee (CGROC):

(i) Exercise its responsibility as a guiding and decision-making forum for SAFRA's operational risk management matters;

(ii) Treat operational risk as a distinct category of risk to be managed in its deliberations;

(iii) Supervise the activities and evaluate the work of the Operational Risk department related to operational risk management;

(iv) Decide on methodologies for capital allocation of operational risk and quantification and monitoring of operational risk appetite;

(v) Submit to Risks Superior Committee (GIR) significant changes or exceptions, in policies and SAFRA's strategies, as well in your systems, routines and procedures, and submit any extrapolation to the levels of operational risk appetite set in the RAS.

Chief Risk Officer (CRO):

(i) Supervise the development, implementation and performance of the operational risk management structure, including their improvement;

(ii) Ensure compliance with the RAS and strategic objectives of SAFRA, the policies, processes, reports, systems and models used in operational risk management;

(iii) Ensure the adequate training of the members of the operational risk management structure, the policies, processes, reports, systems and models used in operational risk management, even those developed by third parties;

(iv) Subsidize and participate in the strategic decision-making process related to operational risk management and capital management, assisting the board of directors.

Operational Risk Department:

(i) Implementation of the operational risk management structure;

(ii) Designing and dissemination of Norms and Policies for operational risk management and capital management for Operational Risk;

(iii) Risk identification - determining the origin of risks and weaknesses in SAFRA’s processes and relevant services performed by third parties;

(iv) Risk assessment and measurement - proposition of Key Risk Indicators (KRI), quantification of expected and unexpected losses and calculation of the capital to be allocated to operational risk;

(v) Risk mitigation - development of control mechanisms and action plans to mitigate identified operational risks and elaboration of business continuity plans;

(vi) Risk control - monitoring of mitigation actions; proposition, implementation and monitoring of control actions; determination of conformity level of processes; and performing back testing;

(vii) Risk monitoring - monitoring of the events of operational loss, the behavior of the Key Risk Indicators, the exposure limits, as well as the existence of internal controls and business continuity plans and risks arising from hiring of critical third party services;

(viii) Information management relatives to operational losses - losses database;

(ix) Coordination of operational loss management committees, identification of root causes, and corrective / mitigation action plans;

(x) Development of economic capital quantification models and methodologies for Operational Risk;

(xi) Elaboration and application stress calculation methodology, in compliance with Circular nº 3.846/17 and Circular nº 3.911/18, as well to Resolution CMN nº 4.557/17, Section II;

(xii) Realize back testing of implemented operational risk control models and systems;

(xiii) Elaboration of short and long-term capital projections in conjunction with the Finance Department;

(xiv) Elaboration of the annual ICAAP report for Operational Risk;

(xv) Indicate which of the outsourced service providers are the most relevant for the operations of SAFRA;

(xvi) Monitoring of the contingency plan containing the strategies to be adopted to ensure conditions of continuity of activities and to limit serious losses arising from operational risk;

(xvii) Training and dissemination of the Operational Risk management culture;

(xviii) Support to the managing departments of products and services;

Business Continuity Management:

(i) Elaborate the Business Continuity Management Policy;

(ii) Ensure the effectiveness of the Business Continuity Management implementation, assigning responsibilities, conducting periodic testing, managing changes to facilities, people, technology or organizational structure;

(iii) Ensure the appropriate level of the organization stability during recovery of critical processes and services, minimizing possible impacts on SAFRA's image or reputation;

(iv) Ensure coordinated and immediate responses in crisis situations;

(v) Ensure validation tests of contingency environments at minimum annual frequency.

Operational Risk and Internal Controls Officer:

Each support and business departments has a Operational Risk and Internal Controls Officer, whit minimum position of Executive Superintendent or, in the absence of this position, for the employee with position immediately below, representing the first line of defense, with the following duties:

(i) Ensure that the risks of the activities under its management are properly identified, controlled, monitored and mitigated;

(ii) Establish fraud mitigation procedures, disseminating them to all those involved in the processes;

(iii) Ensure the correct application of the Risk Mapping and Control Methodology;

(iv) Elaborate the matrix of risks and controls, keeping it updated;

(v) Apply tests to ensure the effectiveness of risk mitigation controls and report their results to the Operational Risks area;

(vi) Ensure the sending of all occurrences and control failures identified to the Operational Risks area;

(vii) Document and keep up to date documentation of policies, standards, procedures and other documents in your area;

(viii) Disseminate the culture of risks and controls in the department(s) under its responsibility, ensuring compliance with internal regulations and regulatory aspects as well as the effectiveness and integrity of controls;

(ix) Monitor and promptly report fraud or suspicion of fraud to the hierarchy and / or Internal Audit, for the appropriate measures, keeping due secrecy.

Business or Operational Departments:

Represent the first line of defense in the operational risks management, with the following duties:

(i) Application of operational risk management methodologies;

(ii) Identification, documentation, registration and communication to the Operational Risk department of all operational losses resulting from failure, deficiency or inadequacy of internal processes, people and systems, or from external events;

(iii) Business management observing Senior Management guidelines, such as the definition of Risk Appetite;

(iv) Information on all occurrences and control failures identified to the Operational Risk department;

(v) Evaluation of the exposure to operational risk arising from the hiring of relevant outsourced service providers, for the regular operation of the institution or in contingency situations;

(vi) Notification to the Operational Risk department of any and all relevant exposure to operational risk.

Capital Management Department:

(i) Monthly assessment of the adequacy of the Basel, Level I and Principal Capital Indices (metrics);

(ii) Monthly valuation of the leverage ratio;

(iii) Annual elaboration of the Business and Capital Plan;

(iv) Verification of capital adequacy based on internal models, performed annually;

(v) Elaboration of the integrated stress test;

(vi) Studies and evaluation of the impacts, possibilities and opportunities of debt issuance (in conjunction with the Treasury) and dividend distribution;

(vii) Evaluation of the impact of stress scenarios on capital levels;

(viii) Application of the capital allocation model and the procedures for calculating the risk-weighted assets (RWA) portion of the calculation of the capital required by the BACEN for operational risk using a standardized approach (RWAopad - ASA 2).

Planning and Control Advisory Department:

(i) Follow up on some indicators related to non-compliance with Operational Risk Management Policies and, according to internal methodology, apply penalties to the variable remuneration of Commercial Areas in order to ensure an adequate alignment of incentives in order for these indicators to be observed by these collaborators.

Operational Risk's Independent Validation:

(i) Perform technical validations of models and methodologies involved in ICAAP.

Internal Audit:

(i) Periodic assessment, independent of the processes related to SRAFRA Conglomerate's risk management and capital management.

Validity: 2019/2020 **Review:** May of 2020