


| | | | |
|---|---|--|---|
|  Organizational Instrument | | | |
| Type: Corporate Policy | | Phase: In effect | |
| Title: CORPORATE RISK MANAGEMENT POLICY | | Number and Version: PI0028 – V.3 | |
| Issuing Department: PK | Approval: DANTE RAGAZZI PAULI - DRPAULI | Duration of the 1 st version: June 25, 2010 | Duration of this version: December 18, 2018 |
| Related Departments (Areas of Influence): SABESP | | Processes: - | |

1. Introduction

The Corporate Risk Management Policy aims at guiding the company towards the practice of risk assessment in the corporate environment and contributing to the improvement of governance and business planning to preservation and generation value to the Company.


2. Objective

- 2.1 Establish guidelines, concepts and competencies for the risk management process according to the methodology defined by Sabesp, based on the international model COSO ERM: Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management, in the norms ABNT NBR ISO 31000 and ABNT ISO GUIA 73.
- 2.2 Consider the risk view in decision making processes, in line with good market practices.
- 2.3 Generate value for the company and improve governance practices in a way that is systematic, structured and integrated with corporate values and guidelines.
- 2.4 Disseminate the culture and promote the performance of risk management in a standardized way in all of the Company's hierarchical levels.


3. Guidelines

- 3.1 The practice of risk management should be in line with the Company's Mission, Vision, Ethical Values and Guidelines, providing full support to the Strategic Planning and its unfolding.
- 3.2 The risk management culture must be disseminated by the functional risk management authority and must be practiced by all the hierarchical levels at the Company.
- 3.3 The work processes must incorporate risk management in a systematic and standardized manner, according to the risk management methodology adopted by Sabesp.
- 3.4 Employees involved in risk management activities must be trained by the functional risk management authority in the methodology adopted by the Company.
- 3.5 Risks should be identified and classified according to their nature and category:

| Nature | Category |
|---------------|---|
| Strategic: | Governance, Political & Economic and Business; |
| Financial: | Accounting, Credit, Liquidity and Market; |
| Operational: | Environmental, Process and Infrastructure, Personnel, Information and Technology; |
| Compliance: | Regulations and Legislation. |

| | | | |
|---|---|--|---|
|  Organizational Instrument | | | |
| Type: Corporate Policy | | Phase: In effect | |
| Title: CORPORATE RISK MANAGEMENT POLICY | | Number and Version: PI0028 – V.3 | |
| Issuing Department: PK | Approval: DANTE RAGAZZI PAULI - DRPAULI | Duration of the 1 st version: June 25, 2010 | Duration of this version: December 18, 2018 |
| Related Departments (Areas of Influence): SABESP | | Processes: - | |

- 3.6 Process risks should be identified, evaluated, treated, communicated and monitored by Departments and Business Units during the execution of their activities, under the guidance of the functional risk management authority.
- 3.7 Corporate risks should be identified, evaluated, treated, communicated and monitored by the risk owner, under the guidance of the functional risk management authority.
- 3.8 The responsibility for the approval and treatment of corporate risks is defined by levels of authority established according to the impact and likelihood of occurrence.
- 3.9 The risk management process must be monitored by performance indicators.
- 3.10 The decision on the controls to be used to reduce exposure to risks should consider the nature and level of criticality.
- 3.11 When assessing the level of criticality and defining the mitigation action plans, the unit responsible for corporate risk should promote broad discussion with the areas involved.
- 3.12 The risk owner should use the results of the evaluations to review the action plans and prepare contingency plans.
- 3.13 The improvement of risk management should occur through cycles of evaluations and reviews and in response to a specific fact.
- 3.14 The functional risk management authority should provide integrated and efficient solutions to support the risk management process.
- 3.15 The effectiveness of the risk management process should be evaluated annually by the Audit Department.
- 3.16 Corporate risks are communicated to stakeholders at the Company's discretion, through the relevant channels and aligned with legislation and good corporate governance practices.
- 3.17 Corporate risks should be monitored by the Board of Directors, Fiscal Council, Audit Committee and Executive Board through periodic reports of activities issued by the functional risk management authority.
- 3.18 The functional risk management authority is the Risk Management and Compliance Department, which is administratively bound and led by the Chief Executive Officer.
- 3.19 The professionals of the functional risk management authority must have access to data and information necessary for the execution of their activities, being responsible for the confidentiality of such information.
- 3.20 The Company's Executive Board must ensure that the necessary resources are adequately allocated to the functional risk management authority to carry out the Company's risk management activities.
- 3.21 The powers of the Board of Directors, Fiscal Council, Audit Committee, Executive Board, Corporate Risk Management Committee, Board of Directors, Risk Management and Compliance Department, other Departments and Business Units are defined in the Appendix 2 of this Policy.

| | | | |
|--|---|---|--|
|  | Organizational Instrument | | |
| | Type: Corporate Policy | | Phase: In effect |
| | Title: CORPORATE RISK MANAGEMENT POLICY | | Number and Version: PI0028 – V.3 |
| | Issuing Department: PK | Approval: DANTE RAGAZZI PAULI - DRPAULI | Duration of the 1 st version: June 25, 2010 |
| Related Departments (Areas of Influence): SABESP | | Duration of this version: December 18, 2018 | Processes: - |


3.22 Those responsible for the risks should implement the mitigation action plans within the established deadline.

3.22.1 If it is impossible to meet the deadline, such fact must be formally informed and an extension to the deadline must be requested to the functional risk management authority, with a copy sent to the respective director.

3.22.2 Mitigation action plans approved and not implemented within the specified period must be informed to the competent departments.


4. Supplementary Items

| Referred Attachments (Attachments Base) | Referred Documents | Record Information |
|---|--------------------|--------------------|
| - | - | - |
| Attached Files (Documents that serve as Supplement to the Corporate Instrument) | | |
| PI0028v3 – Appendix 1 – Definitions | | |
| PI0028v3 – Appendix 2 – Competences | | |

| | | |
|--|---|-----------------|
|  | Appendix Name: | Appendix Number |
| | Definitions | 0001 |
| | Related to Document: PI0028v3 – Corporate Risk Management Policy | |

Description

| | |
|-------------------------------------|---|
| Risk Management | <p>An assessment process that allows an organization to analyze to what extent potential risk factors can impact the achievement of objectives.</p> <p>The Management evaluates events based on two perspectives - probability and impact - and generally uses a combination of qualitative and quantitative methods.</p> |
| Good Corporate Governance Practices | Publicly-recognized guidelines aiming at achieving and maintaining transparency, equity and quality of information, as well as maintaining a positive market reputation and a differentiated position towards the preservation and generation of value. |
| Control | Measure that maintains or modifies the risk. |
| Corporate Risk Management | <p>It is the corporate process conducted by the Board of Directors, Audit Committee, Executive Board, Corporate Risk Management Commission, departments, business units and other employees that is applied towards the establishment of strategies and formulated to identify potential events that can affect the company. Also manages the risks in order to keep such events compatible with the company's risk exposure and provides a reasonable guarantee for the fulfillment of the company's objectives.</p> <p>Risk management is directly related to sustainable growth, profitability, preservation and generation of value for the Company and its shareholders since this process allows the identification of not only threats, but also improvement and development opportunities for the business.</p> |
| Risk identification | <p>Searches for processes, recognition and description of risks. Risk identification involves the description of factors and their potential consequences. Provides a comprehensive list of risks (portfolio) based on events that can create, increase, prevent, reduce, accelerate or delay the achievement of corporate objectives.</p> <p>Risk identification may involve historical data, theoretical analyzes, opinions of informed persons and experts and stakeholder needs.</p> |
| Impact | Result or effect of a risk event. There may be a number of possible impacts associated with an event. The impact of an event may be positive or negative in relation to the Company's related objectives. |

| | | |
|--|---|-----------------|
|  | Appendix Name: | Appendix Number |
| | Definitions | 0001 |
| | Related to Document: PI0028v3 – Corporate Risk Management Policy | |

Description

| | |
|-----------------------------|--|
| Risk Map | <p>A graphical representation of the risk assessment process within the corporate environment. It is presented graphically in a 5 X 5 map layout by positioning the level of risk in quadrant with a corresponding color.</p> <p>Represented on a Cartesian plane with ordered pairs (Probability and Impact):</p> <p>X-axis: Probability: Almost Certain (red), Probable (orange), Possible (yellow), Low (light green) and Improbable (dark green);</p> <p>Y-axis: Impact: High (red), Relevant (orange), Moderate (yellow), Low (light green) and Minimum (dark green).</p> |
| Risk Management Methodology | A set of definitions of identification, analysis, evaluation, treatment and monitoring of risks standards based on the application of the COSO model "Enterprise Risk Management - Integrated Framework", in the ABNT NBR ISO 31000 and ABNT ISO GUIA 73 standards considering the characteristics and peculiarities of Sabesp and its business environment. |
| Hierarchical Risk Level | The company's management positions responsible for making decisions relating to the risk management activities, according to the level of criticality (impact and probability) established in the risk map. |
| Probability | <p>Chance of an event happening.</p> <p>In risk management terminology, the word "probability" is used to refer to the chance of something happening, whether defined, measured, or determined, objectively or subjectively, qualitatively or quantitatively, and described using general or mathematical terms (such as probability or frequency over a given period of time).</p> <p>Source: ISO 31000: 2018</p> |
| Risk Owner | Area responsible for identifying, evaluating, treating, communicating and monitoring corporate or process risks. |
| Corporate Risk | Risk that may compromise the Company's ability to achieve its business objectives. |
| Process Risk | Risk that can compromise process results. |

| | | |
|--|---|-----------------|
|  | Appendix Name: | Appendix Number |
| | Competences | 0002 |
| | Related to Document: PI0028v3 – Corporate Risk Management Policy | |

Description

1. Board of Directors

- a) evaluate and approve the Corporate Risk Management Policy;
- b) be aware of the methodology used for corporate risk management;
- c) verify the effectiveness of corporate risk management and control procedures;
- d) assess and approve the hierarchical risk levels that define responsibilities for the risk approval and treatment;
- e) evaluate and periodically approve the corporate risk map and mitigation action plans under the responsibility of the Board of Directors;
- f) monitor and evaluate the progress of the corporate risk mitigation action plans every six months.
- g) be aware of the results of the effectiveness evaluation of the risk management process carried out by the Audit Department;
- h) be aware of the report on risk management activities.

2. Fiscal Council


- a) be aware of the Corporate Risk Management Policy and its methodology;
- b) be aware of the annual corporate risk management work plan;
- c) be aware of the corporate risk map;
- d) be aware of the hierarchical risk levels that define responsibilities for the risk approval and treatment;
- e) be aware of how corporate risk mitigation action plans are evolving;
- f) be aware of the report on risk management activities.

3. Audit Committee

- a) analyze and provide opinion on the Corporate Risk Management Policy and on the corporate risk management methodology adopted by the Company;
- b) monitor the annual corporate risk management work plan;
- c) analyze and provide opinion on the hierarchical levels responsible for defining risk responsibilities, approval and measures to be taken;
- d) be aware of the corporate risk map;
- e) monitor the evolution of the corporate risk mitigation action plans every six months;
- f) be aware of the report on risk management activities.

4. Executive Board

- a) approve the Corporate Risk Management Policy and submit the policy for approval by the Board of Directors;
- b) approve the methodology used for corporate risk management and submit the methodology for approval by the Board of Directors;
- c) approve the Internal Charter of the Corporate Risk Management Commission;
- d) approve the appointment of the members of the Corporate Risk Management Commission;
- e) assess and approve the hierarchical risk levels that define responsibilities for risk approval and management;
- f) monitor how the corporate risk mitigation action plans are evolving and support its development;
- g) evaluate and periodically approve the corporate risk map and mitigation action plans, submitting to the Board of Directors the risks that exceed the Executive Board's responsibilities;
- h) monitor the evolution of the corporate risk mitigation action plans every six months;

| | | |
|--|---|-----------------|
|  | Appendix Name: | Appendix Number |
| | Competences | 0002 |
| | Related to Document: PI0028v3 – Corporate Risk Management Policy | |

Description

- i) be aware of the report on risk management activities.

5. Executive Offices (including CEO)

- a) know the Corporate Risk Management Policy and on the corporate risk management methodology adopted by the Company;
- b) approve the annual corporate risk management work plan and support its development (exclusively for CEO);
- c) know the Internal Charter of the Corporate Risk Management Commission;
- d) be aware of and monitor the annual corporate risk management work plan;
- e) be aware of the hierarchical risk levels that define responsibilities for risk approval and treatment;
- f) approve the corporate risk of the Executive Office;
- g) submit risks that exceed the Executive Office's responsibilities to the Executive Board (exclusively CEO);
- h) monitor the evolvement of the corporate risk mitigation action plans;
- i) support the execution of risk identification, analyses, evaluation, treatment, communication and monitoring works;
- j) assess and approve the measurement and mitigation action plans of its Executive Office;
- k) appoint a Executive Office representative for the Corporate Risk Management Commission.

6. Corporate Risk Management Commission

- a) assess the Corporate Risk Management Policy and propose amendments;
- b) be aware of the corporate risk management methodology;
- c) assess the Internal Charter of the Corporate Risk Management Commission and propose amendments;
- d) assess the hierarchical risk levels that define responsibilities for risks approval and treatment;
- e) monitor the annual corporate risk management work plan;
- f) assess the proposed risk management culture dissemination at all corporate levels;
- g) monitor the evolution of implementation of corporate risk mitigation action plans every two months;
- h) report the evolvement of the corporate risk mitigation action plans within the Executive Board responsibilities every six months.
- i) monitor corporate risk indicators;
- j) assess of the corporate risk map;
- k) be aware of and monitor the execution of risk identification, analyses, evaluation, treatment, communication and monitoring works within the Executive Offices and Department's responsibilities;
- l) advise the Executive Board on matters related to corporate risk management;
- m) know the resources approved for the implementation of the action plans;
- n) be aware of the report on risk management activities.

7. Departments and Business Units

- a) be aware of and apply the risk management methodology;
- b) be aware of the hierarchical risk levels that define responsibilities for risk approval and treatment;
- c) identify, analyze, assess, treat, communicate and monitor the risks within its responsibilities;
- d) monitor the evolution of implementation of corporate risk mitigation action plans within its responsibilities;
- e) propose to the Executive Board treatment and risk mitigation plans within its responsibilities;
- f) prepare and maintain the risk map of its division updated, along with the Risk Management and Compliance Department

| | | |
|--|---|-----------------|
|  | Appendix Name: | Appendix Number |
| | Competences | 0002 |
| | Related to Document: PI0028v3 – Corporate Risk Management Policy | |

Description

- g) define and monitor risk management indicators;
- h) use the results of risk assessments to prioritize the preparation and/or review of contingency plans.

8. Risk Management and Compliance Department– Functional Authority

- a) disseminate the risk management culture at all corporate levels, pursuant to the Company's Bylaws;
- b) propose and maintain the Corporate Risk Management Policy and Internal Charter of the Corporate Risk Management Commission updated;
- c) train leaders and employees involved in risk management activities to apply the methodology adopted by the Company.
- d) prepare proposals of risk responsibilities and submit them for approval by the Executive Board;
- e) prepare the annual work plan and submit it for approval by the CEO;
- f) implement the annual work plan;
- g) propose measures to support the development of risk management;
- h) propose risk assessment, mapping and classification criteria;
- i) contribute to the development of the corporate risk map;
- j) consolidate and guarantee the distribution of the corporate risk map, according to the defined levels of responsibility;
- k) manage the risk management system with the aim of consolidating the risk assessment results;
- l) monitor the evolvement of action plans and report them to the Corporate Risk Management Commission, Executive Board, Fiscal Council, Audit Committee and Board of Directors;
- m) monitor corporate risk indicators;
- n) advise the Corporate Risk Management Commission;
- o) propose the methodology and execute the internal communication of corporate risks to the areas involved;
- p) align risk management practices with the Company's Mission, Vision, Values and Guidelines;
- q) prepare and monitor the performance indicators of the risk management process;
- r) present periodic reports on risk management activities to the Executive Board, Board of Directors, Fiscal Council, Audit Committee and Corporate Risk Management Commission.

9. Audit Department

- a) assess, annually and systematically, the effectiveness of the risk management process and provide improvement recommendations;
- b) present the result of the assessment of the effectiveness of the risk management process to the Board of Directors;
- c) be aware of the corporate risk map;
- d) consider the corporate risk map when elaborating Sabesp's internal audit work schedule.