	POLICY	PCT 007
	RISK MANAGEMENT AND INTERNAL	Date: 24/06/2022
	CONTROL	Page 1 of 18

1. PURPOSE

The Risk Management and Internal Control Policy, abbreviated as “PGRCI”, aims at disseminating a risk management and control environment culture across all Company levels, guiding its employees as to the actions designed to reduce exposure to risks (uncertainties) with the goal of ensuring that the processes of identification, analysis, assessment, prioritization, treatment, monitoring, communication and management of existing risks, and/or risks that may occur in the future, observe the needs and best practices established by Tupy. It also aims to contribute to the decision-making process, maximize business opportunities through achieving strategic objectives and ensuring compliance with laws, regulations, and internal and external standards.

2. SCOPE

The PGRCI is applicable to all areas, macro-processes, and operations of Tupy S.A., subsidiaries and controlled companies which, directly or indirectly, participate in the Risk Management and Internal Control process, which must be acknowledged and put into practice by the entire workforce of the Company.

It is intended for any area that uses or may use the tools provided by the Risk Management and Internal Control (GRCI) area, as support in the conduction of their processes to reduce exposure to internal or external risks, inherent to Tupy’s businesses.

The Company has a specific policy and standards to address financial, market and credit risks.

3. REFERENCES

The PGRCI is supported by the following documents:

- i. ABNT NBR IEC 31010 – Risk Management – Techniques for the Risk Assessment Process
- ii. ABNT ISO GUIDE 73 – Risk Management – Vocabulary
- iii. COSO's Enterprise Risk Management – Integrated Framework
- iv. COSO's Internal Control – Integrated Framework
- v. CEC – Tupy’s Code of Ethics and Conduct
- vi. DAI 001 – Internal Audit Rules
- vii. Company’s Bylaws

- viii. ISO 31.000:2018 – Risk Management Guidelines
- ix. Tupy's Integrity Policy
- x. *Novo Mercado* Listing Regulation by B3
- xi. The Institute of Internal Auditors – Standards and Guidelines

4. DEFINITIONS

Management: Tupy's management is composed by the members of the Board of Directors and the Statutory Directors.

Risk Appetite: the level of exposure that the Company is willing to accept to achieve its goals and objectives, maintain and create value to shareholders, which is directly related to the Company's strategy. Risk appetite is the acceptable risk variation level, considering the fulfillment of specific Company's goals.

Risk Assessment: an integrated process that includes identifying and analyzing the risks to which the Company is exposed to.

Employees: managers, officers, committee members, full-time employees, interns, apprentices, and outsourced workers.

Risk Management and Audit Statutory Committee (CAE): a body without decision-making or management autonomy, which advises the Board of Directors in the exercise of its duties, focusing on monitoring and assessing risks, business, accounting, and Compliance information.

Executive Committee for Risk Management and Internal Controls (CGRCI): Committee linked to the Statutory Directors, responsible for decision-making, selecting and implementing alternative risk management policies, observing the risk tolerance and appetite parameters defined by the Board of Directors.

Board of Directors (CA): collective body responsible for managing the Company, along with the Statutory Directors, in compliance with the requirements set in the Bylaws and in the current legislations.

Internal Control: process carried out by the governance and management areas, as well as other Company employees, aiming at providing reasonable assurance regarding the achievement of objectives related to operations, disclosure, and compliance, changing the business risks by either reducing the probability of their occurrence or minimizing their negative impacts. It includes planning and all methods and actions taken by the Company to safeguard its assets, check the accuracy and correctness of accounting data, develop efficiency and safety (property, physical and environmental) in its operations.

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

Statutory Directors: collective executive body for management and representation, which oversees regular Company operations according to the strategy and general guidelines outlined by the Board of Directors.

Control Owner: responsible for executing and self-assessing internal controls, implementing and responding to action plans in cases where deficiencies are detected.

Process Owner: responsible for ensuring the performance of risk management activities, reviewing the risk rating and monitoring risk exposure as the first line of defense. The role also evaluates the results of control activities execution and ensures the implementation of action plans.

Risk Owner: person directly responsible for managing the risks associated with operations on the first line of defense, monitoring the execution of controls and implementing corrective measures for their due remediation. The role also supports the definition and implementation of the action plans required for correcting and/or minimizing such risks.

Effect: a deviation from the expected outcome – whether positive and/or negative. Effects may have different aspects (such as financial and performance goals, health, safety, and environmental goals, etc.) and may occur at different Company levels, such as strategic, organizational, project, product, process, among others.

Event: incident or occurrence, whether from internal or external sources to the Company, capable of affecting the achievement of objectives.

Risk Factors: specific occurrences that, individually or combined with others, may generate risks to the business.

Risk Management: structured process for corporate risk identification, analysis, treatment, monitoring and communication to standardize and guide the corporate risk mapping and monitoring process, aligning strategy, processes, people, technology, and knowledge, with the purpose of preserving and creating value for shareholders.

Impact: result or effect of an event to which the Company may be exposed to, regarding its business objectives, before and/or after the respective risk assessment, which may be of a tangible or intangible nature according to the risk appetite.

Uncertainty: state of absence of information, even if partial, related to an event and its understanding, knowledge, the probability of such event occurring and its consequences.

Key Performance Indicators (KPI): metrics that have the purpose of measuring the stage of a process or system, with regular monitoring of the results presented, thereby assisting in the assessment and identification of potential issues or challenges, considering the several goals established by the organization for the activities carried out by its employees.

Key Risk Indicators (KRI): metrics used to determine the potential exposure to a certain risk, monitoring the risk levels of specific Company areas, providing significant information for the achievement of strategic objectives, and indicating the need to take actions in a timelier manner.

Three Lines Model: model designed by the IIA (The Institute of Internal Auditors) emphasizing good governance practices, which establishes that the Company's strategy must be aligned with its mission through the encouragement of proactive actions, clearly and objectively establishing the risk management and internal controls as a management responsibility.

Risk Map: non-exhaustive tool comprehending all Company areas in which the main exposures to risks are documented and require to be periodically assessed and monitored by the Company.

Risk Matrix: a management tool that allows to visually identify risk factors, as well as the combination of their impact and probability, emphasizing what risks should be prioritized and the respective action plans.

Strategic Plan (SP): a corporate instrument that consolidates a fifteen-year vision of the strategies and results envisioned by the company.

Policy: set of Company guidelines regarding a relevant matter, applicable to the Company, its subsidiaries, and controlled companies with personnel. The Policy guides actions at all Company levels.

Probability: used to refer to the possibility of something happening, whether defined, measured or determined objectively or subjectively, qualitatively, or quantitatively, and described using general terms or mathematically.

Process: a set of structured, interrelated and internally aligned activities in all Company areas, which uses process inputs to deliver the intended result to achieve its objectives.

Risk: probability that an event from internal and/or external sources will occur and adversely affect the achievement of the Company objectives; it may cover one or more aspects, including: reputational, strategic, financial, operational, regulatory, integrity, political, technological, systemic, socio-environmental, misconduct and illegal acts.

Strategic Risks: risks associated with strategic decision-making by the Company's senior management to achieve its business objectives, ensuring Tupy's competence or ability to protect itself or adapt to changes in the environment in which it operates.

Inherent Risks: risk that exists prior to risk treatment – absence of any action that could change the impact or probability.

Residual Risks: risk remaining after the process of risk management is carried out by the Company.

Stakeholders: interested parties, comprising all the parties involved with the Company's business and operations.

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

Risk Tolerance: the risk tolerance reflects the Company's risk management philosophy, which corresponds to the percentage of acceptable variations to achieve its objective.

5. GENERAL PROVISIONS

5.1 GUIDELINES

5.1.1 Risk Management and Internal Controls in line with the Corporate Strategy

The guidelines in this PGRCI define and characterize the macro-processes within the Company's Enterprise Risk Management, comprising:

- Strengthening of the Risk Management Culture;
- Definition of roles and responsibilities;
- Standardization of concepts;
- Dissemination of best practices; and
- Promotion of the Company's objectives and creation of value for shareholders.

The risk management activities must be constantly assessed based on the Corporate Governance practices defined by COSO's ERM: 2017 – Enterprise Risk Management Integrated with Strategy and Performance and ISO Standard 31000:2018 – Risk Management Guidelines.

Tupy adopts a risk management model based on the Three Lines concept presented by the IIA (The Institute of Internal Auditors), namely:

- **First line:** represented by managers of business and support areas, who must ensure effective risk management within the scope of their direct organizational responsibilities.
- **Second line:** refers to the Company's control areas, responsible for supporting, monitoring, and questioning issues related to risks and controls, as well as supporting 1st line roles by providing training and technical support on the Risk Management and Internal Control model.
- **Third line:** with an independent and objective action, its purpose is to provide opinions to Governance bodies regarding the risk management process and the effectiveness of Internal Controls.

1 ST LINE	2 ND LINE	3 RD LINE
<p>PROCESS OWNER</p> <ul style="list-style-type: none"> Ensure resources to Risk Owners to implement the actions required for risk mitigation; Revise assessments, inform adjustments to the Matrix and point out unmapped risks to the CGCI; Report the status of action and contingency plans being developed to governance bodies. <p>RISK OWNER</p> <ul style="list-style-type: none"> Assess and ensure that the risk is being mitigated and that Control Owners are performing their duties; Implement prevention and mitigation controls and assign Control Owners; Report deviations to Process Owners. <p>CONTROL OWNER</p> <ul style="list-style-type: none"> Execute controls and action plans. Report deviations to Process Owners. 	<ul style="list-style-type: none"> Analyze, assess and monitor the risks identified by 1st line roles and their accuracy; Assist in identifying risks and developing processes and controls; Provide technical guidance and support; Timely report relevant information related to risk management to governance bodies. 	<ul style="list-style-type: none"> Provide independent and objective assessment and advice on the adequacy and accuracy of governance and risk management to the CAE (Risk Management and Audit Statutory Committee) and on the overall adequacy of the environment to the CA (Board of Directors).

Figure 01

5.1.2 Risk Appetite Statement

Tupy S.A. disseminates a culture of integrity and high ethical standards, and maintains a solid risk awareness, which encourages it to review and contest existing practices. It promotes an organizational environment where challenges are a common part of discussions and decisions on risk-taking. It strictly complies with policies, legislations, regulations, and standards.

It encourages innovation among its employees by means of investments in technology and business, in segments appropriate to its corporate strategy. The Company strives for corporate and socio-environmental sustainability, for the health and safety of its employees and third parties, financial discipline, ethical standards, and the security of its assets.

5.1.3 Good Corporate Governance Practices

Manage risks and internal controls based on the best corporate governance practices, using a structured method that is appropriate to its objectives.

5.1.4 Process Integration

To promote the effective and efficient management of the risk factors present in all the Company's business units and areas.

5.2 RISK MANAGEMENT PROCESSES

5.2.1 Establishing the Context

Understanding the business and its market context includes external (competition, geopolitics, economy, laws, regulatory acts, environment, etc.) and internal (organizational culture, strategic planning, capital structure, financial stability, etc.) factors, forming the basis of information used for identifying, measuring, treating and prioritizing risks.

The Company’s Risk Appetite statement is determined based on parameters from the Financial Impact matrix as a percentage of EBITDA.

5.2.2 Risk Identification

Internal and external risks to which the Company is exposed to are regularly identified, revised and documented in a risk matrix. This step also seeks to identify emerging risks.

5.2.3 Risk Analysis, Assessment, Prioritization and Treatment

Inherent risks – related to operations/business/activities – and residual risks – those that remain or arise after including additional controls and/or adjusting existing ones – are assessed, as well as their probability and impact, in order to support the decision on risk prioritization. Each assessed risk is assigned to an owner, and the result of the combination of Probability and Impact receives a final “A”, “B” or “C” grade, as seen in figure 2.

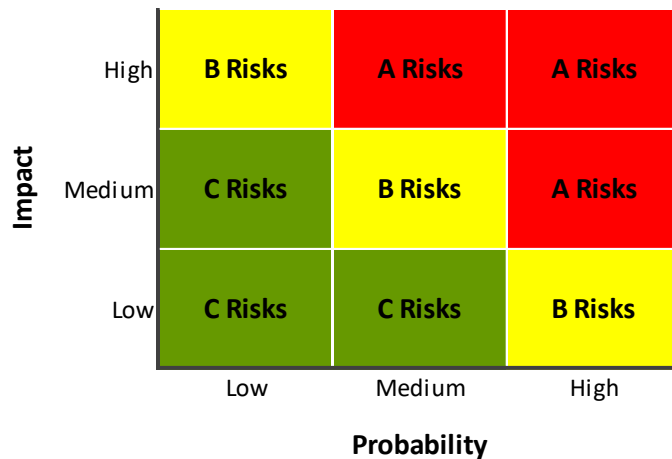


Figure 02

The risks are addressed as follows:

- **“A” Risks:** Account for priority risks that demand immediate action to seek the elimination/mitigation of the risk source by preparing action plans and/or implementing internal controls;

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- **“B” Risks:** Risks of medium criticalness that require attention whose focus should be to define acceptable levels of loss per events, and competence limits that prevent an increase in the impact level over time, by preparing action plans and/or implementing internal controls;
- **“C” Risks:** Risks subject to the implementation of internal controls consistent with their criticality levels.

After conducting a risk assessment, the administration determines how it will respond to the risks. The alternatives for risk treatment are classified as follows:

- a. Eliminate activities that trigger the risk event;
- b. Reduce the probability of the risk event occurring and/or the magnitude of the impact;
- c. Transfer or share part of the risk event; and
- d. Accept the risk event.

5.2.4 Communication

Implementation of continuous processes with interactions with all stakeholders, that allow the information of the results of all steps in the risk management process, to assist in the understanding of risks and the effectiveness of action plans.

5.2.5 Monitoring

The purpose of monitoring is to assess the effectiveness of the risk management process by means of constant management activities and/or independent assessments. It uses continuous verification, supervision, and critical observation to identify changes in the required or expected performance level. The GRCI area is responsible for monitoring and reporting the progress of the action plans for the listed risks.

5.3 INTERNAL CONTROLS

5.3.1 Purpose

The Company's Internal Controls must allow the Administration to monitor operational and financial processes, as well as the risks of non-compliance and discontinuity, according to the policies, standards and limits established by the Board of Directors, providing sustainability and longevity for the Company's business.

Control activities must be constantly assessed, using as a reference the good Corporate Governance practices set out by the standards and methodology of the Committee of

Sponsoring Organization of Treadway Commission – COSO and the Control Objectives for Information and related Technology (CobIT).

5.3.2 Objectives

Tupy's internal controls aim at:

- Promoting operational efficiency, effectiveness, and fulfilment, through the orderly, ethical and cost-effective execution of operations;
- Ensuring compliance with applicable laws and regulations, including standards, policies, programs, plans and procedures;
- Safeguarding and protecting property, assets and resources from waste, loss, misuse, damage, unauthorized use or misappropriation.

The Company's internal control Management applies the following concepts and structures:

- **CSA - Control Self-Assessment:** process carried out by the business areas to assess the design and implementation of internal controls and whether they are being carried out pursuant to their objectives;
- **ToE - Test of Effectiveness:** process of testing the effectiveness of internal controls to certify that they are properly executed by the business areas, allowing the identification of potential gaps;
- **Sign-Off:** process used by the Company's administration to approve the results of internal control assessments.

6. DUTIES AND RESPONSIBILITIES

6.1 BOARD OF DIRECTORS - CA

- a. Approve the guidelines for Tupy's integrated risk management and internal control process (methodology, processes, systems, policy, standards and reporting mechanisms, among others);
- b. Deliberate on the risk appetite in line with the strategic plans;
- c. Approve the prioritized strategic risks and their respective response and contingency plans;
- d. Approve the PGRCI and its revisions;
- e. Approve the Risk Matrix methodology;

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- f. Periodically assess the strategic risk portfolio, Risk Map and the execution of Action Plans for risk mitigation;
- g. Supervise and ensure that the necessary resources are made available for the full operation of the risk management structure and internal control system.

6.2 RISK MANAGEMENT AND AUDIT STATUTORY COMMITTEE - CAE

- a. Advise the Board of Directors in the approval of the strategic risks to be prioritized, their respective mitigation and contingency plans, the changes in the risk criticality, appetite and tolerance assessments, and the definitions of guidelines and policies for the risk management process integrated with internal controls;
- b. Advise the Board of Directors in the analysis of annual and periodic assessments of external audits related to risk management and internal control processes;
- c. Assess the risk management process and structure and the effectiveness of existing controls, to ensure treatment and monitoring of risks;
- d. Monitor the existence of criteria for risk assessment, mapping and ranking, as well as the existence of controls for such monitoring;
- e. Keep track of results and plans for mitigation and contingency actions in risk management and internal control processes and report any recommendations to the Board of Directors;
- f. Oversee the progression of the efficiency level of internal controls;
- g. Monitor the quality and completeness of risk management mechanisms and internal controls.

6.3 STATUTORY DIRECTOR

- a. Assess and suggest updates/changes to the PGRCI;
- b. Ensure that the PGRCI is applied throughout the Company, incorporating risk management practices and internal controls into the decision-making process;
- c. Identify and validate the risks of the respective areas according to the risk appetite and tolerance;
- d. Approve the Annual Plan of the GRCI area;
- e. Review and approve the strategic risk portfolio;
- f. Assign risk and process owners;
- g. Assess the action plans suggested by risk owners and approve any deadline extensions;

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- h. Define expectations regarding integrity, ethical values, transparency and responsibilities for compliance with internal controls;
- i. Monitor the assessments of controls and action plans carried out by the business areas in the CSA process, requesting a timely response to any gaps identified;
- j. Indicate the need for independent assessments of the risk management and internal control process (internal or external agents), to ensure its effectiveness;
- k. Ensure the continuous development of employees working on the Company's risk management and internal controls;
- l. Ensure autonomy for the Company's internal control agents to perform their activities, ensuring access to documents, information systems and people, as well as any other elements required for them to perform their activities;
- m. Ensure the alignment between the Strategic Planning and GRCI, aiming at appropriately managing risks;
- n. Ensure the necessary resources for the carrying out action plans for risks mitigation;
- o. Validate internal control reports issued by the Internal Audit regarding the effectiveness of controls;
- p. Propose the approval of the Company's Risk Matrix.

6.4 EXECUTIVE COMMITTEE FOR RISK MANAGEMENT AND INTERNAL CONTROLS - CGRCI

- a. Analyze and suggest strategies for risk management and internal control processes;
- b. Analyze and present improvement points for the risk management and internal control processes (methodology, processes, systems, policy, standards and reporting mechanisms, among others);
- c. Assist the Statutory Directors in preparing proposals for deliberation by the Board of Directors, regarding the risk appetite;
- d. Assess and deliberate about the risk management work plan for the Statutory Directors;
- e. Assess the authority levels required for risks, which define the responsibilities for risk approval and management;
- f. Identify and analyze the internal controls in business areas, aiming at assessing their effectiveness, sufficiency, and applicability in the mitigation of the risks to which they are related;
- g. Identify, develop, and monitor Key Risk Indicators (KRIs) and monitor Key Performance Indicators (KPIs), always seeking to consider both as tools for risk management and internal controls;

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- h. Assess the risk matrix and internal controls, keeping them always updated and seeking constant improvements;
- i. Supervise the mapping and assessment of risks that may compromise the achievement of the Company's strategic objectives;
- j. Formulate and supervise the method for topics and macro-processes prioritizing, for risk management and implementation of internal management controls;
- k. Monthly keep track of the results of mitigation actions and risk indicators proposed to treat prioritized strategic risks, suggesting guidelines or actions with the purpose of framing, adjusting and mitigating risks that may exceed the tolerance levels;
- l. Periodically keep track of the assessment results of internal control systems of processes;
- m. Analyze and provide recommendations for the portfolio and strategic risk treatment plans whenever updates are made;
- n. Analyze and propose the prioritization of strategic risks;
- o. Analyze and suggest the preparation of treatment plans based on assessments of internal control systems of processes;
- p. Monitor the recommendations and instructions deliberated by the own Committee;
- q. Assess and suggest the resources required to execute risk management and internal control processes;
- r. Ensure compliance with the PGRCI;
- s. Issue opinions on the activities of the Executive Committee, when demanded by the Statutory Directors, , the Audit Statutory Committee and the Board of Directors, preparing, upon request, a technical report on the topics within its competence.

6.5 VICE-PRESIDENCY OF FINANCE AND ADMINISTRATION

- a. Develop and apply tools and mechanisms for risk management and internal controls that are appropriate for the execution of this Policy;
- b. Measure and assess the quality of such mechanisms;
- c. Prepare and submit a proposal for revision of this Policy, whenever necessary;
- d. Promote systematic debates and deliberations in its action forums and alongside different management areas, to ensure the effectiveness of risk management and monitoring;
- e. Coordinate the Executive Committee for Risk Management and Internal Controls (CGRCI):
- f. Ensure compliance with the PGRCI;

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- g. Define the responses to risks (avoid, mitigate, share or accept).

6.6 FIRST LINE

6.6.1 Process Owners

- a. Support the duties and activities of the Risk Owner;
- b. Support the Risk Owner by providing the means to implement the actions required to mitigate risks, ensuring the engagement and appropriate deliverables from participating areas;
- c. Recommend changes to the Risk Matrix when deemed necessary, and ensure that risks are documented in the event that they do not fall under the existing topics of the current Risk Matrix, including significant potential changes to risk probability and/or impact or any other risk attribute, and unmapped risks, if identified;
- d. Revise the criticality of risk (impact versus probability), considering changes in existing mitigation actions, conclusion of action and contingency plans;
- e. Certify (sign off), annually or on demand, that the risks related to the processes under their responsibility are properly identified, assessed, and recorded in the risk management system;
- f. When required, provide reports to governance bodies on the development of risk mitigation and contingency action plans;
- g. Attend regular meetings organized by the GRCI area or governance bodies, upon request.

6.6.2 Risk Owners

- a. Manage the risks under their responsibility, identifying, assessing, treating, preventing and monitoring risks in an integrated manner;
- b. Develop indicators to monitor the variation and results of the risks under their responsibility;
- c. Ensure implementation of the necessary actions to mitigate risks, alongside other business areas, proactively deploying and executing any mitigation or elimination actions deemed necessary, by transferring, sharing, or rejecting risks over acceptable levels.

- d. Prepare systematic reports to present to the GRCI area and the Executive Committee for Risk Management and Internal Controls, regarding the risk monitoring under their responsibility;
- e. Monitor and report for validation by the Process Owner, the results and critical analysis of risk indicators, mitigation actions, as well as updates in the financial impact, following the schedule defined by the GRCI area;
- f. Support the Process Owner and the GRCI area in any significant changes to risk probability and/or impact or any other risk attribute, and unmapped risks, if identified;
- g. Timely inform the Process Owner of the area and the GRCI of events that may change the Risk assessment, as well as assess topics applicable to the Risk Map in the different geographic regions;
- h. Continuously assess the applicability of risk matters in the Risk Matrix for the activities under their responsibility;
- i. Suggest treatment of the Risks for which they are responsible to the Process Owner, who should then forward the suggestion to the GRCI area, and ensure Action Plans are prepared and executed;
- j. Inform to the GRCI area events that may impact the execution of predetermined controls, as well as the need to create new controls to mitigate risks;
- k. Take action regarding the gaps identified, creating and executing required remediation plans;
- l. Implement effective prevention and mitigation controls, ensure the appropriate definition and execution of action plans and establish corrective actions for continuous improvement of risk management;
- m. Ensure compliance with external regulations and internal policies and standards;
- n. For risks that should be continuously monitored, ensure the effectiveness of controls and the timeliness of action plans;
- o. When deemed necessary, request additional support from the process owner to progress in the preventive treatment of the risks under their responsibility;
- p. Meet the minimum guidelines, technical and management standards defined by 2nd Line roles;
- q. Carry out a technical revision of risk, its factors and criticality (impact versus probability), considering changes to existing mitigation actions and the conclusion of action and contingency plans;
- r. Attend regular meetings organized by the GRCI area or governance bodies, upon request.

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

6.6.3 Control Owners¹

- a. Provide data and information to the Risk Owner for a technical revision of the risk, its factors, criticality (impact versus probability) and response, considering changes to existing and proposed mitigation action and contingency plans;
- b. Execute the assigned prevention and mitigation controls, always ensuring accurate and timely information and a secure process, according to the applicable legislation, policies and internal standards and seek the correction of controls, in case any gaps are identified;
- c. Carry out the Control Self-Assessment (CSA) at the frequency defined in the control, providing support and conditions for assessment of internal control systems related to the processes for which they are responsible;
- d. Prepare and execute action plans for controls that they deem to be deficient, or which require implementation;
- e. Timely execute and respond to action plans related to controls.

6.7 SECOND LINE

6.7.1 Risk Management and Internal Controls - GRCI

- a. Continuously support and promote a culture that embraces Risk Management and Internal Controls in the Company, disseminating concepts, knowledge, and good practices at all employee levels;
- b. Propose and revise guidelines for Risk Management and Internal Control processes (methodology, processes, systems, policy, risk portfolio, standards and reporting mechanisms, among others), periodically updating the procedures resulting from this Policy;
- c. Develop, conduct, and apply a methodology to identify, assess and monitor risks and internal controls with the Company's areas;
- d. Propose, to be approved by higher levels of the Company, the Risk Matrix and any reports or analysis resulting from it;
- e. Prepare, revise, and update the risk portfolio whenever updates are made to the Company's risk map or when relevant events occur, reporting to the Statutory Directors, the Executive Committee for Risk Management and Internal Controls and Risk Management and Audit Statutory Committee;

¹ Control owners may also be mapped to second-line roles.

- f. Assist in defining Process Owners, Risk Owners, Control Owners, and other internal control agents, helping them to determine risk indicators, management actions and contingency plans;
- g. Monitor changes to the criticality of strategic risks and report them to the Executive Committee for Risk Management and Internal Controls and Statutory Directors;
- h. Prepare and periodically revise the risk management work plan;
- i. Support the external disclosure of official information regarding the business risk management;
- j. Monitor the elaboration and execution of the action plans required to mitigate risks, along with other Company areas;
- k. Document and assess the design of business processes as to the exposure to risks, identifying opportunities for improvement and the need to implement internal controls;
- l. Support 1st Line roles, by providing training and technical support on the Company's Risk Management model;
- m. Maintain internal controls up to date and in line with the Company's processes, providing support to the areas involved in the CSA, remediation plans and the Sign Off process;
- n. Work with the Statutory Directors, the Executive Committee for Risk Management and Internal Controls, the Risk Management and Audit Statutory Committee and the Board of Directors in deliberations regarding the definition of the Company's risk appetite and tolerance;
- o. Monitor the alignment between the Strategic Planning and Risk Management and Internal Controls, aiming at appropriately treating risks;
- p. Report results on a monthly basis to the Board of Officers and Executive Committee for Risk Management and Internal Controls, and every two months to the Risk Management and Audit Statutory Committee and the Board of Directors;
- q. Ensure that recommendations related to risks and internal controls, made by Internal and External Audits, supervisory bodies and external controllers, are incorporated into the mapping of processes and treatment plans.

6.7.2 Other Areas

Other Company areas – in addition to the GRCl, Occupational Safety, Environment and Compliance – also have 2nd line roles regarding their respective potential risks. These areas have the following duties:

This Policy is to be used exclusively by Tupy. Reproduction without authorization from the issuing sector is prohibited.

- a. Acknowledge, disseminate, and act in compliance with Tupy's corporate Risk Management guidelines;
- b. Define methodologies, minimum technical, technological, and management standards, and risk indicators to be adopted by 1st Line roles;
- c. Support 1st Line roles by assessing the concepts adopted, checking if risks have controls mapped and if the barriers implemented are the best for each situation regarding to the relevant risks;
- d. Assist in identifying risks, assessing the need for additional controls and any non-compliance of existing controls, issue recommendations, and provide technical support in implementing the model and standards for risk and assets management and prevention;
- e. Outline action plans to mitigate the corporate risks under their responsibility, reporting to the GRCI about the treatment and action plans to mitigate risks;
- f. Assess the applicability of standards and indicators by the operational, commercial, project, support, and administrative support areas (1st Line), with independency and transparency;
- g. Add to the agenda of applicable forums potentially relevant risks, in case deliberations on preventive actions requiring additional support are required.
- h. Establish, maintain, promote and assess efficient business practices, and appropriate and effective internal controls;
- i. Document internal controls implemented by the respective Company areas;
- j. Present to the GRCI management, the documentation for the internal controls implemented by the respective areas under their responsibility.

6.8 THIRD LINE

6.8.1 Internal Audit

- a. Certify the effectiveness of controls implemented to mitigate risks (ToE);
- b. Align the audit plan to the business risks;
- c. Report the results of internal control assessments and follow-up of the action plans for identified gaps in internal controls.

7. ACCOUNTABILITY

Any failure to comply with the responsibilities/duties defined in this Policy must be examined by the GRCI area and forwarded for assessment by the Executive Committee for Risk Management and Internal Controls (CGRCI), which will then report it to the Statutory Directors, for the implementation of actions required to determine accountability according to the provisions in the Company's Code of Ethics and Conduct.

Employees in any Company level or area, including stakeholders, who identify any deviation from the guidelines in this Policy, may report it through the Tupy's Ethics Channels.

8. EXCEPTIONS

Exceptions not accounted for in this Policy must be forwarded to the GRCI area to be assessed and subsequently reported to the Executive Committee for Risk Management and Internal Controls (CGRCI).

9. FINAL PROVISIONS

The contents of this Policy may be amended only if approved by the Board of Directors, whenever deemed necessary by such management body or as a result of regulatory changes.

In force: as of June 24, 2022.

3rd version: 06/2022

Area responsible for the document:

Task	Area
Preparation	Risk Management and Internal Controls
Revision	Statutory Directors, Corporate Governance Committee and Risk Management and Audit Statutory Committee
Approval	Board of Directors