

## **RISK MANAGEMENT POLICY**

## 1 OBJECTIVE

Establish guidelines and competencies for risk management, so that business risks can be identified, assessed, prioritized, treated, communicated and monitored. The policy also aims to disseminate and encourage a risk culture at the Company.

## 2 REFERENCES

- Corporate Governance Rules of the Company's Bylaws;
- ABNT NBR ISO 31.001 - Risk Management;
- ABNT NBR ISO 37.001 - Anti-Bribery Management Systems - Requirements;
- ABNT NBR ISO 37.301 - Compliance Management Systems - Requirements;
- COSO ICIF and ERM;
- COBIT;
- NIST.

## 3 INVOLVED AREAS

This policy applies to all collaborators of the Iguá Saneamento Group.

## 4 TERMS AND DEFINITIONS

- **Risk appetite:** Maximum level to which the Company is willing to expose itself in relation to risk(s) in order to meet its strategic objectives.
- **CA:** Board of Directors of Iguá Saneamento.
- **CoAud:** Iguá Saneamento's Audit Committee.
- **COBIT:** Control Objectives for Information and Technology. Guide or set of good practices on corporate information technology governance.
- **Compliance:** Compliance with regulations, laws (fiscal, tax, labor, environmental and others in force for the company), covenants, contracts and standards, procedures, guidelines and internal policies that apply to the business.
- **Internal Controls:** Internal control is a process conducted by the entity's governance structure, management and other professionals, and designed to provide reasonable assurance regarding the achievement of objectives related to operations, disclosure and compliance.
- **COSO:** The Committee of Sponsoring Organizations is a private, non-profit organization created to prevent and avoid fraud in a company's internal procedures and processes through ethics, effective internal controls and corporate governance.
- **Risk Owner:** Member appointed by the Company to monitor and treat the risks assigned to them.

- **NIST:** National Institute of Standards and Technology. Non-regulatory agency that promotes innovation through the advancement of science, standards and measurement technology.
- **Report:** Periodically updating those involved on the situation, assessment, points of attention and response to corporate risk.
- **Risk Response:** Set of measures adopted by the Company to deal with the impact and/or probability of the risk, with the option of avoiding, reducing, sharing or accepting the risk.
- **Risk:** Uncertainty about the possibility of gains or losses for the Company when events related to its objectives occur.
- **Corporate Risks:** Risks arising from the Company's inability to protect itself from events unfavorable to the fulfillment of its strategies.
- **Transactional or Operational Risks:** This is the risk of losses caused by faulty or failed processes, policies, systems or events that interrupt business operations. Collaborators errors, criminal activities such as fraud and physical events are among the factors that can trigger operational risk.
- **SD:** Significant Deficiency.
- **TAR:** Risk Acceptance Term.

## 5 DUTIES AND RESPONSIBILITIES

### 5.1 COMPLIANCE AND INTERNAL CONTROLS MANAGEMENT

- Ensure that the Board of Directors and CEO have access to clear and objective information on the main risks and how these are managed in a timely manner.
- Be the guardian of the Company's risk management methodology.
- Establish and disseminate the risk management methodology in the Company.
- Act as a link between the Risk Owner and the Audit, Risk and Compliance Executive Board, followed by the Audit Committee.
- Transmit knowledge about risks and risk management to collaborators.
- Establish and keep up-to-date the Risk and Internal Controls Policy and Procedures, as well as standards and reporting mechanisms.
- Propose the methodology for calculating risk appetite.
- Calculate and update the risk appetite value annually or when relevant events occur.
- Promote the spread of a risk management culture.
- Assist the Risk Owner in defining or identifying mitigating initiatives and indicators for monitoring risks.
- Maintain and coordinate the updating of the risk matrix.
- Review and update the Probability and Impact Ruler.
- Report the risk matrix and the status of mitigating actions.

- Monitor the Company's risk exposures, the adequacy of response plans and the effectiveness of internal controls.
- Define an internal control work plan based on the processes directly associated with corporate risks.
- Report the results of tests on the controls that mitigate corporate risks.

## **5.2 AUDIT, RISK AND COMPLIANCE BOARD**

- Propose guidelines and strategies for risk management and internal controls.
- Review the work plan for risk management.
- Evaluate the risk matrix and risk treatment.
- Evaluate the progress of risk mitigation actions (action plans).
- Monitor and ensure that changes to the risk criticality assessment are reported to CoAud.
- Communicate to Compliance and Internal Controls Management the existence of risks that have not yet been mapped and dealt with, or a significant change in the probability, impact or any other characteristic of the risk.
- Ensure that the risk matrix is updated with the Company's executives whenever there are updates to the Company's strategic planning or whenever relevant facts occur.
- Understand the methodology for calculating risk appetite.
- Monitor and, when necessary, request updates to the risk appetite.

## **5.3 AUDIT COMMITTEE (CoAud):**

- Validate the guidelines for the structure, governance and process of Risk Management and Internal Controls.
- Propose the Company's risk appetite to the Board of Directors.
- Recommend any changes to this policy to the Board of Directors.
- Supervise internal controls and risk management.
- Understand, evaluate and monitor the risk matrix.
- Report to the Board of Directors on risk levels (high and significant).
- Recommend the improvement of the Risk Management Governance structure (methodology, processes, systems).

## **5.4 BOARD OF DIRECTORS**

- Approve the Company's Risk Management Policy.
- Approve the guidelines for establishing the risk management structure, governance and process.
- Approve the Company's acceptable level of risk appetite.
- Decide on the measures necessary to ensure alignment between the risk appetite and the execution of strategies.
- Periodically assess the risks reported and monitor risk management actions.

- Ensure that risk management and internal control systems are in place to prevent and mitigate the main corporate risks.

## **5.5 RISK OWNERS (BUSINESS AREAS)**




- Carry out a technical review of the risk, the risk factor, the responses and the risk assessment and draw up an action plan.
- Coordinate the implementation of the necessary actions, including the involvement of other areas, in line with the response plan for risk mitigation.
- Develop indicators to monitor the results of the risk under management.
- Make periodic reports to the Risk Management area on the development of risk mitigation actions.
- Assess the risk in relation to its probability and impact.
- Communicate any significant changes in probability and impact or any other characteristic of the risk to the Compliance and Internal Controls area.
- Communicate any changes in controls, initiatives and action plans established to mitigate risks to the Compliance and Internal Controls area.

## **6 DESCRIPTION AND CHARACTERIZATION OF ACTIVITIES (RISK MANAGEMENT)**

### **6.1 GENERAL GUIDELINES**

- 6.1.1 The Risk Management function is a cyclical and dynamic process that identifies, assesses, monitors and responds to risks that could jeopardize the achievement of the Company's strategic objectives or cause significant impacts on its business. This process allows decision-makers at all levels to have timely access to sufficient information regarding the risks to which they are exposed, in order to support decisions and the definition of strategies that increase the probability of achieving objectives and minimize risks to acceptable levels.
- 6.1.2 It is a preventive approach that aims to create the means to manage and keep risks under control (within the established appetite) in order to anticipate possible incidents or crises.
- 6.1.3 There are two distinct and complementary visions of risk management: the Corporate Vision and the Transactional Vision.
- 6.1.4 The Corporate Vision manages risks that affect the company as a whole and are directly related to the Organization's strategic objectives and business continuity.
- 6.1.5 The Transactional View (operational layer) manages risks related to the Company's processes, systems, contracts and business units, considering the specific impact on each area. This type of risk details and complements corporate risks and is associated with them as risk factors, as illustrated below:

Figure 01: Different views of risk management

 <p><b>Estratégico</b></p> 	<ul style="list-style-type: none"> <li>• Eventos que coloquem em risco o alcance dos <b>objetivos estratégicos</b> ou a continuidade dos negócios</li> <li>• <b>Conjunto de Riscos Transacionais</b> que potencializam a materialização de Riscos Corporativos (<b>Fatores de Risco</b>)</li> <li>• <b>Visão Executiva dos riscos</b> da Iguá e suporte para tomada de decisões</li> <li>• <b>Ações</b> de resposta <b>desdobradas por toda</b> Iguá (Top Down)</li> </ul>
 <p><b>Transacional</b></p>	<ul style="list-style-type: none"> <li>• Eventos que coloquem em risco o alcance dos <b>objetivos setoriais</b>, a saúde, a segurança, o meio ambiente e a conformidade de processos</li> <li>• <b>Conjunto de controles</b>, projetos ou iniciativas existentes</li> <li>• <b>Visão operacional</b> e detalhada dos riscos (<b>nível processo</b>)</li> <li>• <b>Ações de resposta restrita às respectivas áreas de atuação</b>, geralmente sem sinergia com as outras áreas</li> </ul>

6.1.6 Risk management is directly related to sustainable growth, profitability, preservation and the creation of value for the Company and its shareholders, since this process allows the identification not only of threats, but also of business opportunities.

6.1.7 An effective risk management process, which is achieved through compliance with good Corporate Governance practices, aims to manage risks effectively, allowing those responsible, at all levels of governance, to have timely access to sufficient information related to risks to which they are exposed, in order to support decisions and definition of strategies that increase the probability of achieving objectives and minimize risks to acceptable levels.

6.1.8 Risk management, through a structured approach and a better understanding of the interrelationships between risks, aligns strategy, processes, people, technology and knowledge, taking advantage of the benefits inherent in diversification, with the aim of preserving and creating value for the Company.

6.1.9 In order to standardize Risk Management at Iguá, it is established that:

- Risk management must be incorporated into the Company's culture and be present in all processes and activities.
- The leadership must promote a risk management culture at all hierarchical levels and in their respective areas of activity, as well as ensuring the application of the principles and adherence to risk management procedures.
- Top Management sets the tone for the entire Company, reinforcing the importance of and establishing supervisory responsibilities for risk management.
- Risk-based decision-making must be incorporated into management, with a view to preserving and creating value for the Company.
- Risk management must be integrated into the Management, Compliance, Internal Controls and Internal Audit processes, promoting the early identification of risks and their conservative and timely management.

- The risks identified must be analyzed and classified by nature, category, the origin of the events (internal or external) and their impact on the organization. If necessary, there should be action plans, with the appointment of Risk Owners and a defined monitoring plan.
- Independence in the risk management process and segregation of duties between risk takers and those responsible for monitoring them must be ensured.
- Continuous monitoring of risks and incorporation into management routines are vital to ensure the effectiveness of risk management and its improvement through frequent evaluation cycles and reviews, with the aim of continuously improving the process.
- Analyses, responses and approvals of **corporate risks**, after assessing their criticality, should be grouped by the following levels:

Levels	
<b>High</b>	Audit Committee and Executive Board
<b>Significant</b>	Management and Executive Board
<b>Moderate or Low</b>	Management

- The analyses, responses and approvals of **transactional risks**, after assessing their criticality, must be grouped by the following levels:

Levels	
<b>High and Significant</b>	Management and Executive Board
<b>Moderate or Low</b>	Management

- Any acceptance of risks of any kind must comply with the provisions of TM-COR-RCI-001 - Risk Acceptance Term - TAR and must be applied to the entire company, including risks identified in internal audits.

## 6.2 STRATEGIC ALIGNMENT AND INTEGRATED MODEL

6.2.1 Risk management is an integral part of the process of drawing up the strategic objectives and is directly aligned with these objectives, establishing an integrated and virtuous cycle of feedback between the Company's lines of defense for broader coverage of internal and external risk factors in the light of the expected results.

6.2.2 The risk management structure supports the integration of governance, at all levels, activities and significant functions, encompassing the most diverse areas and specialties, acting with synergy to protect the business and support leadership in monitoring and timely adaptation of its strategy in the face of any changes in the risk environment.

Figure 02: Three Lines of Defense IIA Model



### 6.3 CONTEXT AND SCOPE

6.3.1 In this first stage, a survey of information and study of the external context (financial, economic, regulatory, socio-environmental environment and relations with stakeholders) and internal context (governance, organizational structure, strategy, processes, systems, contracts, audit reports and other assessments available) to define scope, that is, activities and critical themes that will be subject to mapping, thus arriving at risk scenarios to be better evaluated.

### 6.4 RISK IDENTIFICATION

6.4.1 Based on the outcome of the risk scenario, the risks that could help or hinder Iguá in achieving its objectives are identified, as well as those responsible (Risk Owner).

6.4.2 To find, recognize and describe the risks, Iguá uses interviews with executives and board members, data collection, analysis of evidence, documents, research and validation with the technical areas involved. The result will be a list of risks associated with the scope and scenario defined.



## 6.5 RISK CATEGORIZATION

6.5.1 For categorization purposes, Risks at Iguá should be divided as follows: Strategic, Socio-environmental, Financial, Operational, Regulatory and Technological.

Category	Description
<b>Strategic</b>	These are the risks associated with management's decision-making and which could generate a substantial loss in the Company's economic value. In addition, they can have a negative impact on the Company's revenue or capital as a result of poor planning, adverse decision-making and changes in its business environment. Potential Impact resulting from decisions, due investments and lack of capacity to respond to changes in the environment.
<b>Socio-environmental</b>	Risks of losses in the company's results and balance sheet caused by direct or indirect damage to the environment. Potential impact resulting from the occurrence of an event associated with inadequate management of environmental issues.
<b>Finance</b>	Risk of loss of financial resources by the Company, related to foreign exchange exposures, interest rates and price fluctuations (e.g.lack of adequate approval processes, lack of reconciliation of transactions, operations in foreign currency, commodity prices, reduction in contribution margin, undue access to system transactions, etc.). Potential impact arising mainly from unreliable or misleading financial disclosures.
<b>Operational</b>	Risks of loss resulting from inadequate internal processes, technological failures, human or systems errors, which also includes environmental, social or fraud-related risks. These relate to the Company's infrastructure (processes, people and technology), which affect operational efficiency and the effective and efficient use of its resources. Potential impact resulting from operational problems, such as flaws in internal controls.
<b>Regulatory</b>	Risks related to compliance with legislation applicable to the area in which we operate, as well as general laws (environmental, labor, civil and tax). Potential impact arising from non-compliance with laws or regulations or lawsuits filed by clients or counterparties.
<b>Technology</b>	Risks consisting of the loss, misuse, access or unauthorized disclosure of information or personal data of internal or external stakeholders, which could threaten the Company's business or damage its image.
<b>Image and Reputation</b>	Risks of loss of the Company's image and reputation, such as negative media coverage, loss of market share, causing damage to the company or potentially halting operations. Serious exposure or severe penalties for managers/collaborators, causing irreparable damage to the company's image.

- 6.5.2 In view of the numerous definitions of risks and the need for a common language for all those involved in the process, Iguá has adopted a Risk Dictionary by segmenting risks into categories, subcategories and types of risk, taking into account the company's characteristics and business environment.
- 6.5.3 The breakdowns of the Categories, Subcategories and Types of risks are presented in the Risk Dictionary.
- 6.5.4 The descriptions of the types of risks are presented in document LI-COR-RCI-001 - List of Iguá Corporate Risks Dictionary.

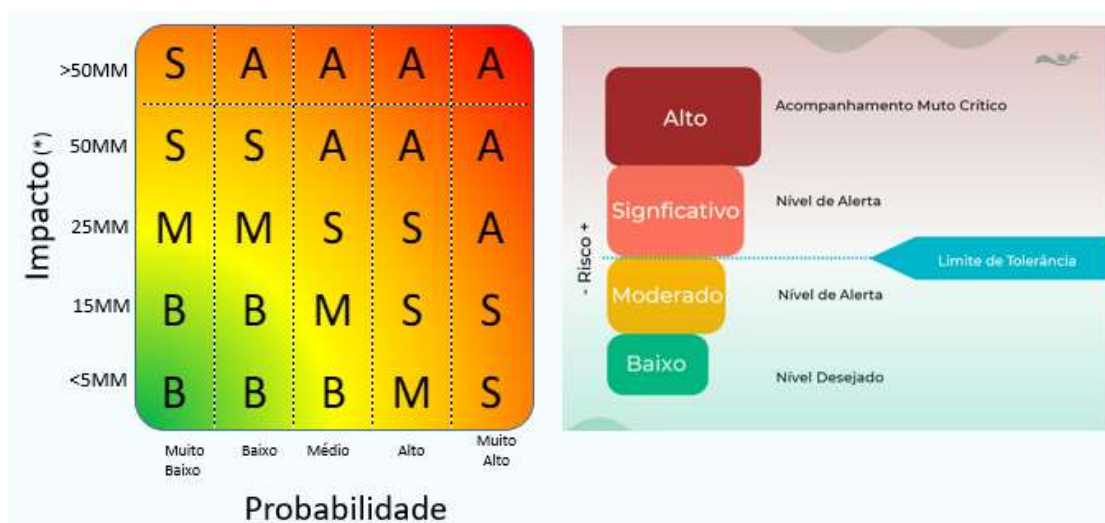
## **6.6 ANALYSIS (IMPACT AND PROBABILITY)**

- 6.6.1 The Compliance and Internal Controls area must assess the impact and likelihood of the risks materializing together with the managers responsible, as well as the assertiveness of these analyses and the effectiveness of the controls and action plans.
- 6.6.2 The risks identified (inherent risk) will be measured considering the level of probability and frequency and impact, as assessed by the Compliance and Internal Controls area in conjunction with the respective risk owners. The final classification of the degree of risk will be defined by a combination of impact and frequency.
- 6.6.3 The risk analysis should determine the Level of Risk Exposure (High, Significant, Moderate or Low) already taking into account controls and initiatives implemented (residual risk).

## **6.7 RISK APPETITE**

- 6.7.1 Risk Appetite is a statement from the highest level of the Organization (Board of Directors) about the extent to which the company is willing to accept risks in order to achieve its objectives. Composed of the "Desirable, Alert and Intolerable" risk levels, it establishes the limits within which the Board expects Management to operate, and determines parameters for risk analysis, as well as serving as a basis for prioritizing and deciding on the appropriate treatment (response).

Figure 04: Heat Map and Risk Appetite



6.7.2 The Heat Map above establishes the risk classification based on an analysis (real or estimated) of probability (chance of materialization) and impact (in R\$MM). Alongside this, Appetite defines the risk tolerance limit as cases with a "High" and "Significant" level of risk exposure not being tolerated.

6.7.3 In addition to the quantitative aspects resulting from the impact and probability analysis, qualitative parameters such as professional judgment and the following assertions are also considered in the Appetite:

- Iguá does not tolerate non-compliance and/or misconduct by executives, collaborators or third parties with applicable laws, rules and regulations;
- Iguá does not tolerate operational negligence that affects its customers' service levels;
- Iguá does not tolerate waste of resources and acts that may cause damage to its assets, those of third parties, public assets or the environment; and
- Iguá does not tolerate negative exposure of its brand that could affect its image, reputation, business activities and stakeholders.

6.7.4 The analysis of the financial vector is based on the Company's EBITDA result, according to the financial impact rule:

Below are the values updated to the accounting EBITDA of December/2022.

Mínimo	Baixo	Moderado	Significativo	Alto
Impactos financeiros negativos no caixa abaixo de R\$ 5 milhões.	Impactos financeiros negativos no caixa entre R\$ 5 e R\$ 15 milhões.	Impactos financeiros negativos no caixa entre R\$ 15 e R\$ 25 milhões.	Impactos financeiros negativos no caixa entre R\$ 25 e R\$ 50 milhões.	Impactos financeiros negativos no caixa acima de R\$ 50 milhões.
~ 0 a 1%	~ 1 a 3%	~ 3 a 5%	~ 5 a 10%	~ Acima 10%

## 6.8 RISK CLASSIFICATION AND MONITORING

6.8.1 The risk management process includes not only identifying risks and risk factors, but also classifying and monitoring their treatment. In this way, after analysis, the risks identified are classified as "High", "Significant", "Moderate" or "Low", with "High" and "Significant" risks being monitored by Top Management and the Board. The "High" and "Significant" risks are monitored by the Top Management and the Board in fixed and recurring agendas at their ordinary meetings or at extraordinary meetings to ensure timely deliberation of any risks and factors considered urgent and relevant.

6.8.2 The classification is defined through the evaluation and application of a set of probability criteria (history of occurrence or estimated projection of the possible materialization of risk factors) and impact (potential consequences arising from the occurrence of the risk), considering:

- Planning and strategic objectives;
- Parameters proportional to the size of the Company, updated periodically;
- Comprehensive quantitative (not just financial) and qualitative vectors;
- Risk Appetite (defined by Management and the Board according to each specific risk); and
- Mitigating controls and initiatives (residual risk).

6.8.3 The details of the methodology and classification criteria, as well as the mechanisms for responding to and monitoring risks are set out in the procedures (PR-COR-RCI-001 - Risk Management and Internal Controls Procedure), duly approved and in line with market standards and best practices.

## 6.9 RISK TREATMENT AND RESPONSE

6.9.1 The Business Areas must develop preventive and corrective actions to respond appropriately, effectively and mitigate the Company's risks:

Risk Response	Description
<b>Accept</b>	<p>This strategy is adopted when it is not possible or practical to respond to the risk using the other strategies. When Top Management decides to accept the risk, it means that they are agreeing to face the risk if and when it occurs. An emergency contingency plan or palliative solution plan should be developed for this eventuality.</p> <p>Actions are usually defined to deal with all the risks identified, or whose final assessment was below the expected residual risk. Exceptionally, a TM-COR-RCI-001 - Term of Acceptance of Risk- TAR is approved on a reasoned basis and in accordance with the governance and competent authority established in PR-COR-RCI-001 - Risk Management Procedure. This is an "agreed" formalizing that there</p>

	<p>will be no action/initiative due to, for example, technical or financial unfeasibility, cost x benefit of the solution, among other factors.</p> <p>It is worth noting that TAR does not apply to cases where the level of risk exposure is above the Company's Risk Appetite or where audits have indicated a Significant Deficiency (SD).</p>
<b>Share/Transfer</b>	It involves finding another party that is willing to take responsibility and bear the impact of the risk, should it occur (e.g. insurance, bonds and guarantees).
<b>Avoid</b>	The risk can be avoided by removing the cause of the risk or by carrying out the operation in a different way, but still in line with achieving the company's objectives. Not all risks can be avoided/eliminated, and this approach can be costly.
<b>Reduce / Decrease</b>	Risk mitigation reduces the probability and/or impact of an adverse risk event to an acceptable limit (expected residual risk) by implementing controls and initiatives. The implementation of control and/or initiatives can take place immediately or within defined timeframes through established action plans.

6.9.2 At this stage, the best options for responding to the risk should be selected and implemented, the effectiveness of this response assessed, a decision made as to whether the remaining risk is acceptable and, if applicable, additional treatments carried out. The benefits, costs, efforts, advantages and disadvantages of implementation must be balanced. If possible:

- Carry out additional analyses to better understand the risk;
- Improve existing controls and initiatives, and assess the need for new implementations;
- Hiring insurance to share risks and monitored retention;

6.9.3 For more details on risk response mechanisms (controls and initiatives), see PR-COR-RCI-001 - Risk Management and Internal Controls Procedure.

## 6.10 TERM

6.10.1 The Transactional Risk Matrix will be reviewed annually in the current cycle or in due course when necessary.

6.10.2 The Corporate Risk Matrix (Iguá Saneamento e Operações) will be reviewed biannually or when the need arises.

## 7 FORMS/TEMPLATES

- LI-COR-RCI-001 - Iguá Risk Dictionary List
- MP-COR-RCI-001 - Sanitation Value Chain Map – Iguá

## 8 ANNEXES

Not applicable.