AZUL S.A.

PUBLICLY-HELD COMPANY

CORPORATE TAXPAYERS' REGISTER (CNPJ/ME) N. 09.305.994/0001-29

BOARD OF TRADE (NIRE): 35.300.361.130 – CVM 24112

CORPORATE RISK MANAGEMENT POLICY OF AZUL S.A.

1. Purpose:

The purpose of this Corporate Risk Management Policy ("Policy") is to establish guidelines, principles and responsibilities to support all business areas in the process of identification, assessment, treatment, monitoring and communication of the Risks and opportunities to which the Company is exposed, with an overall vision.

2. Application:

This Policy applies to all companies and business units of the group Azul S.A., including its affiliates ("Company") and it members (including the chief executive officer, executive officers, directors, managers, employees and interns, as well as all members of the board of directors, collectively referred to as "Crewmembers").

3. Normative References:

The legislation, regulations and other instruments listed below, as eventually amended, revoked or updated, integrate and complement the provisions of this policy, as applicable:

- Safety Management Manual (2018 Edition) – ICAO Doc 9859;
- ABNT NBR ISO 31000 Standard – Risk Management: Principles and Guidelines;
- COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management—Integrating with Strategy and Performance (2017);
- COSO – Committee of Sponsoring Organizations of the Treadway Commission - Internal Control – Integrated Framework (2013);
- Institute of Internal Auditors of Brazil – Models of the three lines of defense;
- CVM Normative Instruction No. 586/17 – Brazilian Code of Corporate Governance - Publicly-held Companies;
- M-ERP-001 – Emergency Response Plan;
- MP-TIN-005 – Cyber Crisis Response Plan.

4. Definitions:

- **Action plan:** Action (or set of actions) aimed at reducing risk exposure.
- **COSO (Committee of Sponsoring Organizations of the Treadway Commission):** Private, non-profit organization dedicated to improving financial reporting, especially

through the application of corporate risk management, fraud prevention and effectiveness in the application and compliance of internal controls.

- **Impact**: The extent to which a risk event might affect the enterprise. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer, and operational impacts.
- **Inherent Risk**: Natural risk level in a process that has not been controlled or mitigated in risk management.
- **Internal controls**: Continuous control processes and activities, adaptable to a company's structure, which seek to provide a degree of confidence capable of supporting the achievement of objectives related to operations, reporting and compliance.
- **Likelihood**: Possibility of an event occurring. In relation to risk, likelihood is used to find out the chance of a risk materializing.
- **Residual Risk**: Risk that remains after efforts to identify and eliminate some or all types of risk have been made.
- **Risk**: Events that may compromise the achievement of the Company's strategies and objectives or operates its processes.
- **Risk Assessment**: Process of risk identification, analysis and evaluation.
- **Risk Exposure**: Represents the combination of impact and probability of loss or other potential adverse effect arising from the Risk.
- **Risk Owner**: Person or entity with the accountability and authority to manage a risk.
- **SOX (Sarbanes-Oxley Act)**: United States law, signed in 2002 and mandatory for publicly traded companies. It aims to ensure the creation of reliable audit and security mechanisms, in order to mitigate risks to the business, prevent the occurrence of fraud or ensure that there are means of identifying them when they occur, ensuring transparency in the management of companies.

5. Guidelines:

5.1 ROLES AND RESPONSIBILITIES

5.1.1 Board of Directors

- Approve and when necessary revise this Policy;
- Deliberate on the strategic issues of the risk management process, such as the acceptable risk exposure limit and monitor the risks with the support of the committees;
- Approve, when necessary, exceptions to risk management strategies, guidelines and procedures;
- Disseminate the risk management culture among stakeholders of the Company.

5.1.2 Audit Committee

- Assist the Board of Directors in supervising Risk management activities, ensuring that the guidelines are followed;
- Periodically review the Corporate Risk Matrix, deciding on the necessary measures to ensure alignment between risk appetite and strategy execution of the Company;
- Recommend to the Board of Directors, when necessary, exceptions to the Risk management strategies, guidelines and policies;

5.1.3 Executive Board

- Commit to Risk management, allocating the necessary resources to the process, regarding with the guidelines of this Policy;
- Ensure adherence to the acceptable limits established for the Company's exposure to Risks;
- Disseminate the Risk management culture in the Company.

5.1.4 Risk Management and Compliance

- Define the corporate risk management methodology with an integrated and systemic view that enables continuous risk monitoring;
- Ensure maintenance and annual review of the risk management policy;
- Consolidate, evaluate, monitor, and communicate the company’s (strategic, financial, operational and Compliance) risks to the Audit Committee and the Board of Directors;
- Assist business areas in identification and impact assessment of the Risks and in the preparation and updating of action plans to mitigate identified Risks;
- Report information about the Integrated Risk Matrix to the Audit Committee and the Board of Directors, considering the status of controls and business risk action plans;
- Disseminate the risk management culture in the Company, by providing training.

5.1.5 Business/Corporate Areas

- Directly manage the risks, following the guidelines of this Policy: identification, assessment, treatment and monitoring of the Risks, with the Risk Management and Compliance area support;
- Implement and execute effective preventive and mitigation controls, ensure appropriate definition and execution of action plans and establish corrective actions for the continuous improvement of risk management;
- Continuously assess the applicability of risks in the Integrated Risk Matrix to the processes and activities under their responsibility.

5.2 Guidelines

Corporate Risk management is a commitment assumed by the Company, with a focus on

preserving its objectives and contributing to its continuity, maintaining a robust and integrated governance model, for the benefit of its stakeholders (shareholders, customers, suppliers, investors, crew, society and government).

Corporate activities and processes that may generate significant Risks to the business are considered in the Annual Risk Assessment, which is conducted by the Risk Management and Compliance area, together with the business areas. The identified risks, impact and probability criteria are formalized and periodically monitored in the Company's Corporate Risk Matrix.

The management of Risks and opportunities is an ongoing process, and it is the responsibility of all Crew Members, at all levels, to know the Risks in their area of operation and manage them in accordance with the concepts, guidelines and directions contained in this Policy.

5.2.1 Risk Management Structure

The Company uses for the Risk management structure, the model of the three lines of defense proposed by the Institute of Internal Auditors - (IIA 2020), prepared with the purpose of clarifying the roles and responsibilities related to the activities of Risk management and controls, as shown in figure 1.

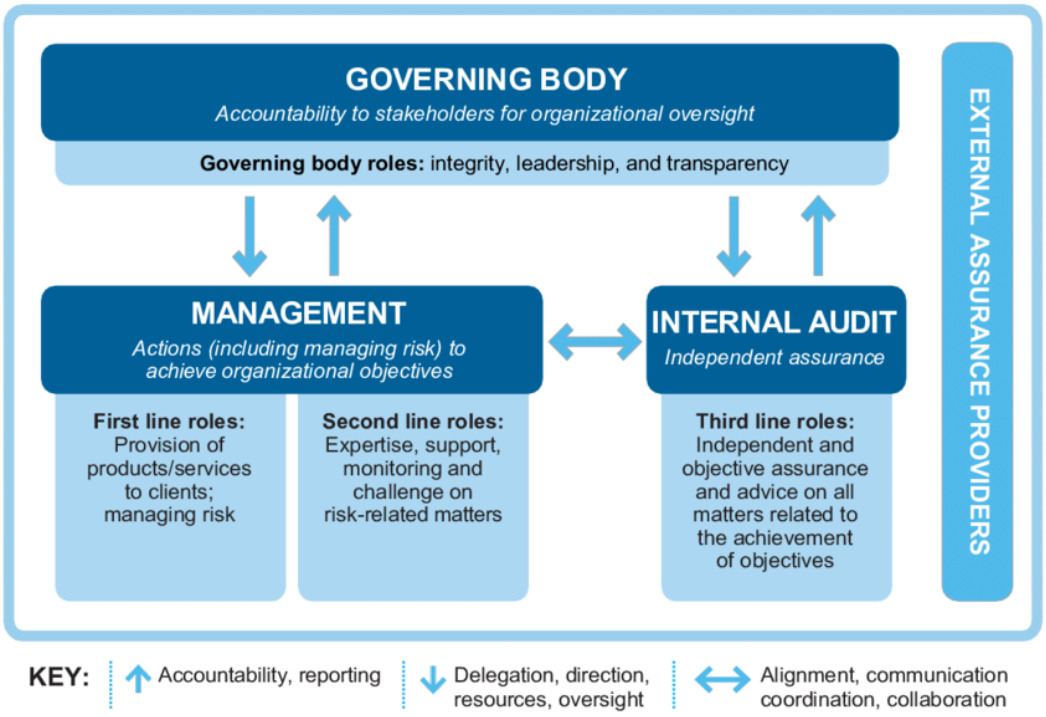

Figure 1. The IIA's Three Lines of Defense Model (2020)

The governance body promotes an integrity, transparency and leadership culture, and must delegate responsibilities and offer resources to management to achieve the Company's objectives. At Azul, it is represented by the Board of Directors and the Audit Committee, determining the organizational appetite for Risks and exercising oversight of Risk management.

The first line of defense is made up of the operational corporate business areas, since the Internal Controls incorporated into the work processes are carried out under their responsibility.

The second line of defense is composed of the control structure, characterized in the Company by the Risk and Compliance Management, which must equip first-line managers for the correct management of Risks and opportunities.

The third line of defense comprises the Internal Audit, which provides an independent and objective assessment and audit of the adequacy and effectiveness of governance and risk management, in addition to reporting weaknesses in the internal control environment, promoting and facilitating continuous improvement.

External assessment providers (such as the external audit) provide additional assessment for the business, aiming to comply with legislation and regulatory expectations.

5.2.2 Methodology

The Risk Management and Compliance area uses as a reference the integrated risk management structure suggested by COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), which defines that an internal control structure must include interrelated components, considering all processes, sub-processes, activities and units of the Company.

The methodology establishes a set of principles (Figure 2) that guide the way in which the Company can design, implement and maintain the structure of internal controls, strengthening risk management associated with Azul's strategies and objectives.

Figure 2. COSO *Enterprise Risk Management* (2017)

The definition of levels, impact and treatment of the Company's corporate Risks is based on document 9859 - *Safety Management Manual* (2018 Edition) made available by the ICAO *(International Civil Aviation Organization*). Although this methodology is directed to the management of operational safety Risks, the levels of Probability, Impact and Risks are adapted to each corporate process of the Company, in search of a unit of Risk assessment and reporting.

5.2.3 Risk Management

I. General Risk Analysis (AGR)

The AGR reflects, the executives' perceptions in relation to the main aspects and characteristics of management and risks involved in the Company's business areas/processes.

Internal or external risks that may impact Azul's business strategies and objectives are identified and monitored to ensure that any materializations that may occur are known and managed to an acceptable level.

The AGR shall be periodically updated in order to identify possible changes in the business environment that may affect the fulfillment of business objectives. Any changes identified must be recorded in the Company's Corporate Risk analysis document, according to the methodology.

The General Analysis of Corporate Risks is composed of the components of the following topics (II to V).

II. Risk Identification and Dictionaries

The purpose of identifying Risks is to find, recognize and describe events that may prevent the Company from achieving its objectives and/or not meeting its obligations.

In order for Risks to be identified, Azul's Risk Management and Compliance area periodically recognizes, documents and formalizes, in a structured manner, together with the business areas, the risks to which the Company is exposed.

The potential corporate risks identified in this assessment are documented through the Risk Dictionary and are classified and categorized in a common language, considering the Company's business characteristics:

- **Strategic Risk:** Consists of the Risks associated with the strategic decisions of the Company's Senior Management, which, due to changes in the internal and external environment (political, technological, economic, social, among others), may impact its ability or ability to protect itself or adapt to changes in the environment in which it operates.
- **Environmental Risk:** Potential damage to the environment and society, caused by the Company's activities, generating an impact on the protection of human, cultural or environmental health.
- **Credit Risk:** Consists of the risk of recurring losses due to default by customers and partners (travel agencies, marketing agencies, representatives).
- **Liquidity Risk:** Lack of availability of sufficient cash resources to meet the Company's liability obligations, such as loans, financing, debentures, salaries, provisions, social charges payable, accounts payable and other liabilities. It may also be related to the difficulty of redeeming invested resources, without losing their value.
- **Market Risk:** Possibility of losses that may be caused by changes in the behavior of interest rates, exchange rates, stock and commodity prices.

- **Operational Risk:** Possible loss of efficiency and/or effectiveness in the Company's operations, due to inadequacy of internal processes, policies, people or systems, which may result in accidents or financial losses.
- **Regulatory Risk:** Exposure to legal penalties, which may generate financial or image losses, due to non-compliance with external and internal laws or regulations (including their updates) that delimit the sector's performance. Such as *the Sarbanes -Oxley Act* (SOX), General Personal Data Protection Act (LGPD - Law n. 13.709/2018), Anti-Corruption Law (Law 12.846/2013), among others.
- **Cybernetic/Technological Risk:** Threats that aim to exploit the Company's vulnerabilities, and that may result in the leakage of information or data belonging to the Company. For example, data from individuals (Customers or Crew members) and legal entities (Suppliers, Third Parties or the Company itself), or commercial and sensitive information. Impacting confidentiality, integrity and availability.

STRATEGIC					FINANCIAL		
ESG*		BUSINESS MODEL		POLITICAL AND ECONOMIC	CREDIT	MARKET	LIQUIDITY
01. Adherence to Policies and Procedures	06. Dependence on personnel	10. Competition and market	14. Organizational Structure	18. Political and governmental context	20. Default	23. Foreign Exchange	27. Cash Flow
02. Communication and dissemination	07. Sustainability	11. Planning and Budget/Management Indicators	15. Business continuity	19. Economic Scenario	21. Chargeback	24. Commodities (Oil)	28. Loans Financing
03. Relationship with Shareholder	08. Organizational Culture	12. Development of the network	16. Investments and projects		22. Unavailability	25. Derivatives	
04. Reputation and Image	09. Social Responsibility	13. Pricing (Revenue Management)	17. Customer satisfaction			26. Interest Rate	
05. Fraud and Unethical Conduct							

OPERATIONAL			REGULATORY		TECHNOLOGY
PROCESS		PEOPLE			
29. Marketing Channel	36. Third Parties and Business Partners	42. Training	45.Regulation (SEC and CVM)	50. Civil	54. Technological Innovation
30. Failures in the Provision of Services	37. Operational Security	43. Availability of labor	46.Regulation (ANAC and others)	51. LGPD	55. Cyber Threats and Attacks
31. Crew Schedule	38. Efficiency	44. Talent Hiring and Retention	47. Accounting and Finance	52. Corruption	56. Infrastructure
32. Airworthiness	39. Business Practices		48. Labor	53. SOX	57. Access/Confidentiality
33. Flight Delay or Cancellation	40. Operational Infrastructure		49. Tax		58. Credibility/Integrity
34. Supply	41. Accounts Receivable and Accounts Payable				59. Availability of Technical Resources
35. Loss or Obsolescence					60. Dependence on IT Personnel

* Environmental, Social and Governance

Figure 3. Risk Dictionary

Once identified and categorized, the Risks are mapped and formalized in the Company's Corporate Risk Matrix. For aeronautical operational risks, there is a specific matrix created and managed by the Quality and Operational Safety Board (Safety).

IV. Risk Map

The risk map shows the exposure of each risk, that is, its classification according to impact and likelihood, considering the perception of the Company's executives and mappings with the business areas. The degree of exposure should be graded in four levels, as detailed in figures 4 and 5.

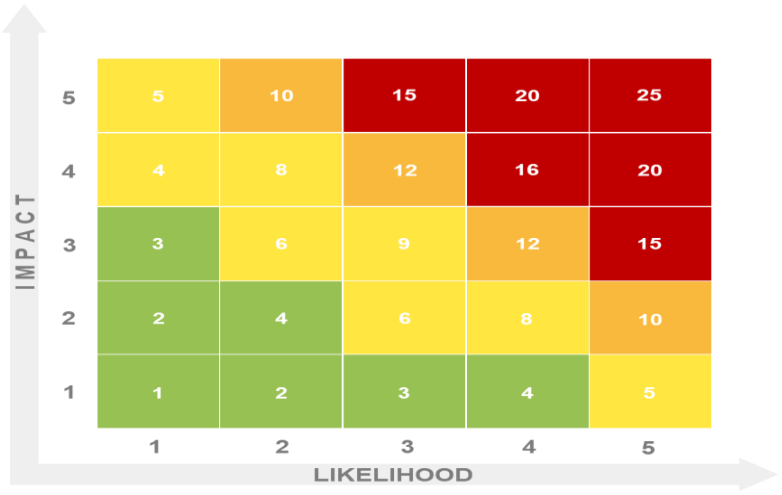

Figure 4. Risk Map

Risk Level	Evaluation Rating	Management	Recommended Action
Extreme	25, 20, 16 e 15	Intolerable	Immediate need for mitigation or termination of activity
High	12 e 10	Tolerable (within mitigation)	Priority in mitigation
Medium	9, 8, 6, 5 e 4	Tolerable	Mitigation
Low	4, 3, 2 e 1	Acceptable	Mitigation measures are not mandatory

Figure 5. Risk Management

The risk exposure framework refers to the extent to which the Company is exposed or unprotected in relation to negative impacts after evaluating existing controls.

V. Criteria for assessing the level of risk exposure

From the understanding of each Risk, the measurement of its level of exposure is carried out by the Risk and Compliance area, in the calculation of the impact x likelihood attributed and its result will present the level of inherent risk identified.

A. Impact Assessment

In the impact dimension, some criteria for qualitative and quantitative assessment are considered as assessment premises, as shown in figure 6.

Impact Rating	Description of Evaluation Criteria	Description of Evaluation Criteria (R$ mil)
Extreme	• Financial losses that may compromise the profitability of the business; • Loss of key customers or market share; • Payment of high fines or severe penalties with an impact on the company's image and reputation; • Loss of large investments or much lower than expected return.	Amount involved above 0.75% of net operating revenue.
High	• Significant financial losses; • Loss of customers or a large number of transactions; • Payment of high fines or severe penalties; • Loss of great business opportunities or investments with an indefinite payback period.	Amount involved from 0.75% of net operating revenue.
Medium	• Considerable financial losses; • Customer dissatisfaction may result in lost transactions; • Payment of fines and other penalties; • Loss of business opportunity; • Failure to comply with internal procedures, laws and regulations.	Amount involved from 0.05% of net operating revenue.
Low	• Intangible financial losses; • Customer dissatisfaction; • Payment of fines and other minor penalties.	Amount involved from 0.01% of net operating revenue.

Figure 6. Criteria for Impact Assessment

The impact classification (Extreme, High, Medium or Low) must start from the definition of the type of analysis, that is, whether the impact will be measured from the qualitative or quantitative category.

The risk category can be evaluated exclusively qualitatively, given the unavailability of a history of materialization of risk or value at risk. The analysis will be quantitative, and the financial value will be considered in its entirety for purposes of framing the impact scale, when the risk has a materialization history or an adherent and concise value at risk.

B. Likelihood Assessment

In the case of likelihood, professional judgment is used to determine a prior assessment of this dimension, considering aspects such as:

- **Control effectiveness:** Control performed or monitored improperly/incompatible with the frequency and design defined in the Action Plan and/or in the Risk Matrix/Internal Controls, increasing the likelihood;
- **Response to materialization of risk:** The absence of a timely and effective response to the materialization of a risk can increase likehood;
- **Complexity or volatility of activities:** The number of factors and volatilities interrelated with aspects such as people, processes, systems and business units, including geographic dispersion of operations. High complexity increases the likelihood;
- **Level of change in processes (growth/contraction):** Recent or future changes in key people, organizational structure, processes, systems, business model or infrastructure increase the likelihood;
- **External conditions:** Volatility of competitive, financial and economic conditions. High volatility increases the likelihood.

The analysis of the likelihood, relative to the level of risk exposure, considering the perception of the executives, the history of occurrence, degree of implementation of the action plans, the current structure of controls and the professional judgment, base the classification of risks in the dimension of the likelihood according to the following rating:

Likelihood Rating	Description of Evaluation Criteria
Extreme	The Company's lines of defense are insufficient to minimize the risk, due to the absence of key controls or the recurrence of problems.
High	The Company's lines of defense are insufficient to minimize the risk, due to ineffectiveness and existing controls, or the recurrence of problems.
Medium	Existing controls do not operate in a standardized way or are ineffective and may not minimize risk.
Low	Existing controls minimize risk.

Figure 7. Criteria for Likelihood Assessment

VI. Risk Treatment

After measuring the Risks, they will be classified for the necessary treatment based on the analyzes of the responsible areas and the definition of acceptable limits for the Company's exposure to Risks:

- **Mitigate:** Adopt measures to reduce the likelihood or impact of exposure to Risks, or both;
- **Avoid:** Promote actions that avoid/eliminate the effects and/or consequences;
- **Transfer:** Reducing the likelihood or impact by transferring or sharing a part of the Risk (for example, taking out insurance, hedging transactions or outsourcing activity);
- **Accept:** Do not initiate any action, maintaining existing practices and procedures, but continue to monitor.

The treatment of Risks is a dynamic and continuous process and when the definition is to mitigate, transfer or avoid Exposure to Risk, Action Plans will be defined by the Risk and Compliance area, together with the areas involved in the process (" *Risk Owner* "), with a view to implementing the necessary controls in response to the risk.

The strategies outlined with the business areas will be registered in the Corporate Risk Matrix as an Action Plan. And the priority for implementing this Action/Control Plan will be measured according to the result of the assessment of each risk. These controls must reduce exposure to the Identified Risk, leading to Residual Risk.

VII. Risk Monitoring

After the adequacy and effectiveness of the implemented controls, for the Risk management to be effective, those responsible (Risk and Process) for the controls must continuously monitor the Risks.

It is important that monitoring takes place in all aspects of the Risk management process, in order to ensure that controls are effective and efficient in both their design and operation, and to obtain information that can improve the Risk Assessment process.

The performance and results of the process must be analyzed periodically by the managers of the areas, in order to identify possible corrections or changes that impact the action plans, and periodically by the Internal Audit.

5.2.5 Business Continuity Management and Crisis Management

The contingency, crisis management and recovery plans consist of immediate measures to be taken by the Company, in the event of materialization of any Risk event. The Emergency Response Plan (M-ERP-001) and the Cyber Crisis Response Plan (MP-TIN-005) are the documents implemented by the Company on the subject.

The documents contain directions, roles and responsibilities of the teams involved, so that critical processes can fully function again, or in an acceptable way, in the shortest possible time, avoiding prolonged interruptions that could generate greater losses, aiming at the best way to resume the affected operations.

***

Barueri/SP, May 5, 2022.