

## **PADTEC HOLDING SA**

### **CORPORATE RISK MANAGEMENT POLICY**

#### **1. Purpose**

This Corporate Risk Management Policy ("Policy") of Padtec Holding SA ("Company" or "Padtec") aims to stipulate the guidelines, principles, roles and liabilities in the management of corporate risks, as well as the development, dissemination and implementation of the of Risks management culture, by guiding the processes for identifying, analyzing, assessing, treating, monitoring and communicating the mapped Risks, aiming at promoting continuous improvement for the Company's processes and obtaining better results.

This Policy also covers the Company's controlled and affiliated companies, especially Padtec S.A.

#### **2. Scope**

This Policy applies to all macro processes, business operations, and areas of the Company, and compliance by management, by the Statutory Audit and Risk Committee members and all Padtec's employees is mandatory.

#### **3. Definitions**

"Action Plan" - is the organized form, according to a certain methodology previously defined by the Internal Controls and Internal Audit areas, as the case may be, which describes goals and objectives, as well as the activities that must be carried out for the treatment of a certain identified Risk to avoid it, accept it, reduce it, eliminate it or transfer it.

"Company" - is Padtec Holding SA and its subsidiaries, especially Padtec SA.

"Controls" - are the actions taken by the Company aiming at reducing the risks inherent to the activities carried out by the business units and other areas, and these activities may be periodic or continuous. These actions will assist the respective bodies of the Company and its employees, as the case may be, in monitoring the exposure levels of each of these Risks.

"Event" - is the occurrence or change in a specific set of circumstances that result in the materialization of a Risk.

"Management" - Board of Directors and Executive Board of the Company.

"Probability" - indicates the possibility of a given event occurring. It can be expressed in quantitative terms, such as percentage, frequency of occurrence, or other numerical metrics, or in qualitative terms, such as high, medium, low.

"Risk(s)" - are the factors and/or events that may cause negative impacts, compromising the Company's ability to achieve its strategic objectives and the effective creation and protection of its value.

"Risk Analysis" - is the process of understanding the nature of a certain risk and determining the Probability of its materialization, resulting in how much the Company would be exposed to that particular risk.

"Risk Appetite" - is the level of Risk exposure that the Company is willing to accept to achieve its objectives within the limits established by the Management.

"Risk Assessment" - is the process of comparing the results obtained in the Risk Analysis with the criteria established by the Management, under this Policy, to determine whether the Risk and/or its magnitude are acceptable or tolerable by the Company.

"Risk Management" - is the set of coordinated and structured activities to align the Risk Appetite with the strategic decision-making cycle in the search for risk mitigation and optimization of the results to be achieved by the Company.

"Risk owner" - has the definition in "Step 2" of item 7 of this Policy.

"Risk Treatment" - is the process of modifying the Risk, which may be the action of (i) avoiding the Risk by deciding not to initiate or discontinue the activity that gives rise to the Risk; (ii) assume or increase the Risk, in order to seek an opportunity for the Company; (iii) removal of the Risk Source; (iv) changing the Probability; (v) changing the expected consequences; (vi) sharing the Risk with other party(ies); and/or (vii) the retention of the Risk due to a conscious choice by the Company.

"Source of Risk" - are the elements that, individually or in combination, have the intrinsic potential to give rise to a given Risk.

#### 4. Duties and Liabilities

FUNCTION	LIABILITIES
<b>Board of Directors</b>	<ul style="list-style-type: none"> <li>• Establish general Risk guidelines aligned with the Company's business context and strategic planning cycle;</li> <li>• Establish, based on the Company's capacity and tolerance, acceptable Risk Appetite limits;</li> <li>• Evaluate, deliberate, and approve the strategic and prioritized risk matrix, aligned with the Company's Risk Appetite;</li> <li>• Define and review Risk Management criteria and strategies;</li> <li>• Annually assess the sufficiency of the Internal Audit area's structure and budget for the performance of its roles, as recommended by the Audit Committee;</li> <li>• Evaluate and deliberate on the reports prepared by Internal Audit, through the Statutory Audit and Risk Committee;</li> <li>• Review and approve the general definitions of Risk Management strategies;</li> <li>• Ensure the Statutory Audit and Risk Committee has operational autonomy and approval of its budget to cover operating expenses – which will be included in the Company's annual general budget;</li> <li>• Approve and modify this Policy, as well as its future developments and revisions.</li> </ul>
<b>Statutory Audit and Risks Committee</b>	<ul style="list-style-type: none"> <li>• Monitor the activities of the Internal Audit and Internal Controls areas of the Company;</li> <li>• Assess and monitor the Company's Risk exposures;</li> <li>• Propose to the Board of Directors the definitions and guidelines to compose the Company's Risk Management model;</li> <li>• Propose to the Board of Directors the tolerance levels for Risk exposure;</li> <li>• Monitor and support the Risk Management process in defining prioritized Risks aligned with the business context and the guidelines of the Board of Directors;</li> <li>• Supervise Risk Management activities in compliance with current legislation and the Company's internal policies, standards, and procedures;</li> <li>• Periodically assess, monitor, and inform the Board of Directors about the prioritized Risks identified by the Risk Owners' reviews in the Risk Management process, assisting in the evaluation of action plans and preparation of recommendations;</li> <li>• Evaluate, approve, and monitor the execution of the treatment and monitoring of Risks;</li> <li>• Evaluate, approve, and recommend to the Management the correction or improvement of the Company's internal policies;</li> <li>• Evaluate the Company's quarterly information, interim statements, and annual financial statements;</li> <li>• Submit to the Board of Directors, for deliberation, the reports prepared by the Internal Audit;</li> <li>• Make recommendations, annually, to the Board of Directors, on the sufficiency of the structure and budget of the Internal Audit area.</li> </ul>
<b>Executive Board</b>	<ul style="list-style-type: none"> <li>• Promote the integration and culture of Risks in the Company and the management and strategic planning cycles;</li> <li>• Ensure the implementation of an efficient Risk Management model, aligned with the Company's objectives and goals. Apply the general guidelines established by the Board of Directors to assign the level of Risk Appetite acceptable to the Company;</li> <li>• Monitor the Risks managed at the level of each process and ensure the effectiveness of the Control measures;</li> <li>• Participate in the validation and prioritization rituals of the Company's Risks with the Statutory Audit and Risk Committee;</li> <li>• Evaluate and monitor the Treatment of Risks aligned with the execution of the Company's strategic planning;</li> <li>• Timely assess the effectiveness and applicability of the guidelines of this Policy;</li> </ul>

	<ul style="list-style-type: none"> <li>Assess and support the adaptations of the structure intended for the Risk management process, considering human, financial and technological resources; and</li> <li>Monitor, assess and supervise the activities of the 1st and 2nd Line of Defense.</li> </ul>
<b>Compliance</b>	<ul style="list-style-type: none"> <li>Guide the analysis of third-party risks to mitigate possible risks of corruption, fraud, conflicts of interest, and negative media, ensuring compliance with current anti-corruption laws and regulations, according to the matrix of prioritized risks;</li> <li>Monitor the risk analyses carried out based on the level of risk classification;</li> <li>Assist in the preparation and adaptation of standards, policies, and procedures to reduce exposure to business risks; and</li> <li>Disseminate the culture of compliance, through training and communications, ensuring compliance with existing laws and regulations, the Code of Ethics and Conduct, and other internal standards and procedures, seeking to mitigate the risks identified.</li> </ul>
<b>Internal Controls</b>	<ul style="list-style-type: none"> <li>Support other areas of the Company in implementing improvements to Controls and processes;</li> <li>Support other areas of the Company in implementing Action Plans and remediating issues identified in the Risk Management process;</li> <li>Support internal and external audits; and</li> <li>Support other areas in improving Controls and processes.</li> </ul>
<b>Risk Management</b>	<ul style="list-style-type: none"> <li>Ensure the operationalization of Risk Management;</li> <li>Execute Risk mapping; and</li> <li>Support other areas of the Company in identifying and assessing Risks.</li> </ul>
<b>Leaders in support and business areas (back office and front office)</b>	<ul style="list-style-type: none"> <li>Identify, classify, and manage the Risks of the respective areas according to the mitigation strategies, together with the Internal Controls area;</li> <li>Indicate the professional who will act as a Risk Management facilitator for the Internal Controls area;</li> <li>Report on the levels of exposure, Action Plans, and indicators that describe the status of the Risks for which they are responsible;</li> <li>Have technical knowledge of the processes in which the Risks are inserted;</li> <li>Be responsible for updating the information on the mapping and treatment of the Risks of their business unit;</li> <li>Keep the information updated promptly, respecting the planning calendar of the Risk Management cycle; and</li> <li>Monitor the status of the Action Plans with those responsible for implementing the Control devices.</li> </ul>
<b>Internal Audit</b>	<ul style="list-style-type: none"> <li>Assess the quality and effectiveness of the Company's Risk Management, Control and Corporate Governance processes;</li> <li>Identify and identify opportunities for improvements in Internal Control and Risk Management processes;</li> <li>Periodically report to the Statutory Audit and Risk Committee and its audited clients the results of independent, impartial, and timely assessments of the effectiveness of Risk Management in the Company;</li> <li>Prepare the planning and ensure the operationalization of Risk Management;</li> <li>Prepare and operationalize the Internal Audit plan, by sector of the Company, by the risks previously mapped and prioritized;</li> <li>Assess the efficiency of Internal Controls, measuring the potential impact and probability of eventual failure of Controls;</li> <li>Assess and propose Control strategies; and</li> <li>Support the areas in implementing improvements in Controls and internal processes.</li> <li>Review and support the preparation of standards, policies, and procedure manuals linked to the processes being audited; • Monitor and control the follow-up of the main points reported in the internal audits.</li> </ul>

<b>All employees of the Company</b>	<ul style="list-style-type: none"> <li>• Ensure the operationalization of Risk Management, being part of the identification, evaluation, and measurement process, and implementing preventive and corrective actions; and</li> <li>• Participate in training that allows the conscious dissemination of the Risk Management culture.</li> </ul>
-------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

The Company's Risk management structure will be led by the following areas/responsible parties, in addition to counting on the effective participation of the members of the Statutory Audit and Risk Committee, the Board of Directors, and the Board of Directors:

- Compliance: This role is performed by the Legal Department and General Secretariat, whose occupant is the Company's Compliance Officer, reporting to the Board of Directors;
- Internal Audit: This role is performed by the Internal Audit area, reporting directly to the Presidency and the Statutory Audit and Risk Committee;
- Internal Controls: This role is performed by the Internal Controls area, reporting to the Information Technology/Corporate Quality management, which in turn is subordinate to the Chief Financial Officer.
- Risk Management: This role is performed by the Strategic Planning area, reporting to the person responsible for the Controllship area, who in turn is subordinate to the Chief Financial Officer.

## 5. Company Guidelines and Lines of Defense

This Policy has as its general guideline the commitment to the Company's value proposal, which, in line with the other corporate policies and the Code of Ethics and Conduct, seeks to create an efficient and integrated Risk Management culture, involving Management and all employees in the process of identifying, assessing and mitigating the identified risks.

Risk Management is part of the Company's corporate governance structure, integrates the decision-making process and contributes to the execution of it

strategy. Risks are identified and treated in order to ensure compliance with the goals established for each strategic planning cycle.

Therefore, the Risk Management structure considers the joint performance of the corporate governance and management bodies, in accordance with the concept of the three lines of defense, according to the competencies described below:

- **1st Line of Defense (Leadership - *front and back offices*)**
  - Includes Operational Management, represented by the Executive Officers, managers and other employees of the business units allocated in day-to-day operations and tasks.
  - Employees working in the 1st Line of Defense have ownership over the Risks and are responsible for implementing corrective actions in order to resolve deficiencies in Control and processes, mitigating the Risks related to the activities they perform.
  - These employees play a crucial role in supporting the 2nd Line of Defense in the process of identifying risk mapping, as well as in the process of executing the Action Plans defined by the Risk Management and Internal Controls area or by the Internal Audit area.
  - Managers are responsible for managing the Risks inherent to the processes under their responsibility from the identification, assessment, monitoring and treatment of these Risks, with the participation of the other areas to be involved, according to the division of competences provided for in this Policy.
  - Report to the 2nd Line of Defense (Risk Management, Internal Controls, and Compliance area) about the Risks inherent in the activities carried out by the 1st Line of Defense that are not yet covered by Controls that mitigate their probability of occurrence and/or impact.
  - Implementation and monitoring of Action Plans to address deficiencies identified in the respective processes.
  - Report of the occurrence of materialization of Risks to the 2nd Line of Defense (Risk Management, Internal Controls, and Compliance area) immediately for treatment and preparation of Action Plans.



## ■ **2nd Line of Defense (Risk Management, Internal Controls, and Compliance areas)**

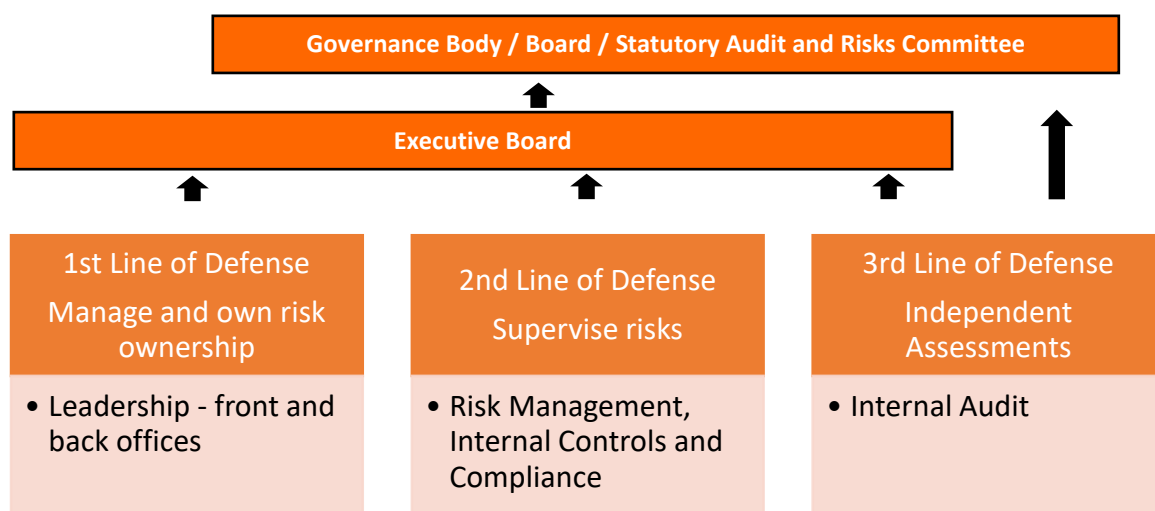
- The 2nd Line of Defense has a preventive status concerning Risks, with an emphasis on internal controls and compliance with laws and regulations applicable to the Company, as well as concerning controllership aspects, with the monitoring of financial risks and financial reporting issues.
- It must guide, monitor and evaluate the adherence to the defined standards and policies and support the 1st Line of Defense to achieve the objectives established by the Company.
- It must advise the 1st Line of Defense on the aspects of internal controls, procedures, rules, and support management policies, define roles and responsibilities, identify changes in the Company's Risk Appetite, assist in the construction of processes, Controls and procedures.
- Facilitation, communication and monitoring of Risk Management practices and assistance in the identification of Risks according to the Risk Appetite established by Management.
- Assessment of the vulnerability of the Controls environment of the Company's processes through effectiveness tests.
- Monitoring the implementation of the Action Plans for the identified failures.
- Preparation of Risk Management planning.

## ■ **3rd Line of Defense (Internal Audit area)**

- It provides the Company's Management and governance bodies with structured assessments of the mapped Risks, based on the events and related consequences, independently and objectively within the Company.
- In a detective way, it provides assessments on the status of governance, structured internal controls and how this scenario impacts the Company's objectives, having in its scope the assessment of efficiency and effectiveness of the operation, safeguarding assets, reliability of information, integrity processes, adherence to laws, regulations, policies and procedures, and analysis of processes in the Company's business and support areas.
- Elaboration and operationalization of the internal audit plan, by Company area, according to the Risks previously mapped and prioritized.

- Assessment of the efficiency of internal controls, measuring the potential impact and probability of eventual failure of the Controls. Deficiencies in Controls should be linked to deficient controls, and managers of the responsible areas are recommended to create Action Plans to mitigate the respective risks.
- Identification of Lack of Internal Controls, with recommendations to managers of the responsible areas to create action plans, which result in the development of internal controls to mitigate the respective risks.
- Identification of general notes on the audited processes, with recommendations to managers of the responsible areas to create action plans to mitigate the respective risks.
- Monitoring of Action Plans on deficiencies, absence of internal controls, and general notes, identified by Internal Audit.

Below, follows the model of three lines of defense adopted by the Company:



## 6. Risk Categorization

The Risks to which the Company is exposed are categorized to standardize internally and externally the references to the various Risks that may impact its activities. The categorization of Risks facilitates the division process according to the respective natures, due also to the segments in which the Company operates that are affected by the Events in a different way.

In this sense, the Company categorizes its Risks as follows:

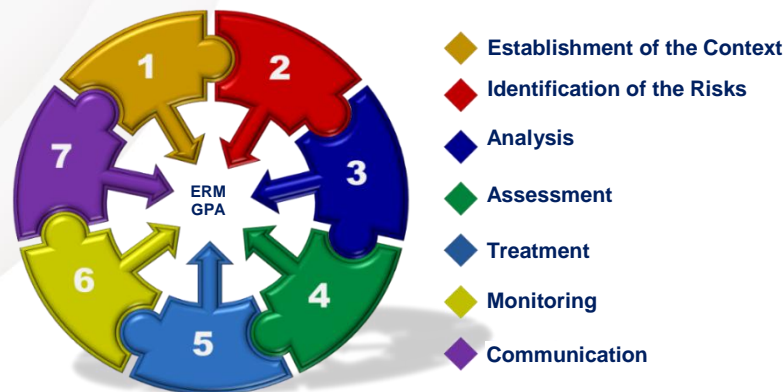


RISK CATEGORY	DESCRIPTION OF RISK CATEGORY
<b>STRATEGIC</b>	Risks associated with decision-making by the Company's Management, the materialization of which may generate a substantial loss of economic value, capital, or market share of the Company, as a consequence of flawed planning and/or decisions, usually related to business strategies/market share, investments, succession, innovation and competition. They are, therefore, Risks that may harm the core of the Company's business model. They challenge the logic of strategic choices, threaten competitiveness, and impair the ability to achieve or maintain exceptional performance.
<b>OPERATIONAL</b>	<p>These are risks arising from failures in processes and controls, lack of consistency and adequacy of information systems, as well as those arising from errors or fraud that impair or prevent the exercise of the Company's activities. Operational risks generally result in the reduction, degradation, or interruption, in whole or in part, of the Company's activities, with possible negative reputational and financial impacts, in addition to the potential generation of contractual, regulatory, and environmental liabilities.</p> <p>In addition, they also include financial risks that may adversely affect the Company's finances, associated with the exposure of financial operations and related to changes in the values of its assets and liabilities, non-compliance with financial obligations of counterparties, high cost or inability to meet financial obligations, inefficiency in capital allocation and failures in financial reporting.</p>

## 7. Risk Management Process

The Company's Risk Management process was defined based on the guidelines of the COSO - Committee of Sponsoring Organizations of the Treadway Commission and the ISO 31000: 2018 - Risk Management Principles and Guidelines.

In this context, the Risk Management process is an ongoing process and an integral part of the development of the Company's activities, incorporated into the organizational culture and practices and adapted to the business processes, consisting of the following subsequent and dependent steps:



## ◆ Step 1: Establishing the context

Initial phase of the ongoing Risk Management process, which articulates the Company's strategic objectives with the external and internal parameters that will be taken into account, establishing the scope and the Risk criteria for the rest of the process.

It seeks to understand the business scenario and context considering factors linked to the Company's short and long term strategic planning, in line with the environment in which these objectives are inserted.

It is a fundamental step to ensure that the Risk Management process is aligned with the Company's management and strategic planning cycles to align its acceptable levels of Risk Appetite.

In order to establish the scenarios that should support this step, the influencing factors of both the External Context and the Internal Context are considered.

### External Context

The External Context is the external environment in which the Company seeks to achieve its objectives. It includes, but is not limited to: (a) cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; (b) key factors and trends that have an impact on the organization's objectives; and (c) relationships with external stakeholders and their perceptions and values.

Generally, the Company is unable to intervene directly on the External Context, having a predominantly reactive action. However, following the guidelines of this

Policy, the Company must seek to mitigate any impacts of Events materialized in the External Context.

## Internal Context

It consists of the Company's internal environment, based on the Company's organizational culture, processes, structure and strategies, at the following levels, but not limited to: (a) culture; (b) rules, guidelines and models adopted by the Company; (c) governance, organizational structure, roles and responsibilities; (d) policies, objectives and strategies implemented to achieve them; (e) capabilities, understood in terms of resources and knowledge (for example, resources, time, people, processes, systems and technologies); (f) information systems, information flows and decision-making processes (formal and informal); (g) relations with internal stakeholders, and their perceptions and values; and (h) contractual relationships.

The attention to the Internal and External Contexts can help to ensure that Risk Management is appropriate to the circumstances, the Company and the Risks that truly impact considering the real scope of its strategic objectives.



## **Step 2: Risks Identification**

The Risk identification approach is top-down, based on interviews with the main executives of the business units, in view of the main processes for which they are liable.

The product generated in this step is a comprehensive list of Risks based on events that may identify vulnerabilities and threats that put the achievement of the Company's strategic objectives at risk.

In this step, the owner and the person responsible for each of the identified Risks (Owner of the Risk) must also be defined, as well as a description that will guide the next steps of the mapping.

Still at this step, all the Risks associated with the Company's activities are mapped, whether these are under its Control or not.



## **Step 3: Risk Analysis**

After completing Stage 2, the identified Risks are analyzed in detail, with the aim of obtaining greater clarity and qualitative and quantitative support that generate

variables that will assist in classifying the Risks so that the Company can act more assertively in its prioritization and the preparation of Action Plans.

At this stage, the causes or factors of Risks are defined, among others, as well as their possible effects in the event of a given Event materializing. In addition, the Company classifies the aggravating factors of each of the Risks identified to ensure the assertiveness of its Controls.

In this way, information is collected with the objective of obtaining data that can describe the probability, impacts, and classification of the identified Risks, thus generating a qualitative matrix to executively describe the universe of Risks based on their classifications. Within the qualitative matrix, Risks are classified according to the following criteria:

IMPACT	QUALITATIVE ASPECTS	PROBABILITY	QUALITATIVE ASPECTS
<b>HIGH</b>	<ul style="list-style-type: none"> <li>- Impact greater than 5% of annual net revenue, compromising the company's financial sustainability;</li> <li>- Total or significant interruption of operations, affecting the production chain and the delivery of products or services to the market;</li> <li>- Serious breach of regulatory standards, which may result in severe penalties, high fines, or restrictions on operations;</li> <li>- Significant negative exposure in the media, loss of trust among customers and stakeholders, compromising the company's credibility.</li> </ul>	<b>HIGH</b>	<ul style="list-style-type: none"> <li>- The event has already occurred in the recent past or occurs frequently.</li> <li>- There are significant gaps in existing internal controls or the absence of preventive controls.</li> <li>- There are no formalized and updated processes, policies and procedures;</li> <li>- Evidence of a history of fraud, errors, or non-conformities related to the risk in question.</li> </ul>
<b>MEDIUM</b>	<ul style="list-style-type: none"> <li>- Impact between 1% and 5% of annual net revenue, causing significant financial adjustments, but without irreversibly compromising operations.</li> <li>- Partial interruption of operations, with manageable impact within reasonable timeframes;</li> <li>- Non-conformities that result in moderate sanctions or require significant adjustments to avoid future impacts;</li> <li>- Moderate exposure, with impact on market perception, but capable of mitigation with strategic actions.</li> </ul>	<b>MEDIUM</b>	<ul style="list-style-type: none"> <li>- The event has occurred in the past but without frequent recurrence.</li> <li>- Internal controls are implemented, but with flaws or opportunities for improvement.</li> <li>- There are formalized processes, policies, and procedures, but they are out of date.</li> <li>- The risk may be triggered by internal or external factors under certain conditions.</li> </ul>
<b>LOW</b>	<ul style="list-style-type: none"> <li>- Impact of less than 1% of annual net revenue, with minimal financial</li> </ul>	<b>LOW</b>	<ul style="list-style-type: none"> <li>- The event has never occurred or there are rare records of occurrence.;</li> </ul>

IMPACT	QUALITATIVE ASPECTS	PROBABILITY	QUALITATIVE ASPECTS
	repercussions that can be absorbed by the company's normal operations; - Minor operational disruption, with no significant impact on the delivery or quality of products and services;  - Payment of fines or other minor penalties; - One-off and short-term impact, with no significant consequences for the corporate image.		- Internal controls are robust, tested, and considered effective; - The risk depends on exceptional circumstances to occur. - There are no formalized processes, policies, or procedures; - Audit and review history does not indicate failures or relevant problems.

Thus, the Risk analysis involves developing an understanding of the Risks mapped in Step 2. Based on this understanding, Step 4 of Risk Assessment is reached and decisions are made about which treatments to be adopted, as well as which strategies and methods are most appropriate for their management.

After defining the impact and probability of the Risk, its classification is automatically generated, which can be LOW, MEDIUM, or HIGH. According to the matrix below:

P R O B A B I L I D A D E	A L T A	MÉDIA	ALTA	ALTA
	M É D I A	BAIXA	MÉDIA	ALTA
	B A I X A	BAIXA	BAIXA	MÉDIA
		BAIXO	MÉDIO	ALTO
		IMPACTO		

Next, the groups must be assigned. In a Risk analysis, Risk groups are categories that group similar types of threats that can impact the business in different ways. This categorization helps in the identification, assessment, and management of Risks in an organized manner, allowing the Company to adopt effective measures to mitigate or control these Risks.

In the Company, the Risk groups are divided into:

**Access:** Refers to the risks associated with the management of permissions and access control to information, systems, and facilities. It serves to protect sensitive data and ensure the security of the technological and physical infrastructure of the Company and its businesses. It is important to highlight that the Company has a Privacy and Personal Data Protection Policy that meets and complies with all the requirements of the General Personal Data Protection Law (LGPD), Law no. 13,709, of August 14, 2018.

**Administrative:** Involves risks related to failures or inefficiencies in administrative and managerial processes, such as communication problems, inadequate human resource management, and poor management decisions. It is paramount to ensure efficient operation and internal compliance.

**Customs:** Covers risks associated with import and export processes, including compliance with customs regulations and the collection of fines. If these risks are not properly mitigated, they may lead to operational and legal problems and financial losses. Failure to effectively manage these risks may compromise the costs and delivery times of the Company's products to end customers and the maintenance of the Authorized Economic Operator (AEO) Certificate, which is essential for the continuity of its foreign trade operations. To ensure compliance with current legislation and the preservation of the AEO Certificate, Customs Risks are strictly monitored by the designated manager and are subject to frequent audits conducted by the Internal Audit area.

**Environmental:** Includes risks related to environmental impacts and sustainability, such as natural disasters, pollution, and changes in environmental regulations. Serves to mitigate negative consequences and maintain compliance with environmental laws and the Company's actions towards society.

**Cyber:** Refers to digital security threats, such as hacker attacks, data leaks, and malware. Essential to protect the integrity and confidentiality of the Company's data and that of its stakeholders when shared with the Company.

**Customer:** Risks related to the behavior and expectations of customers and potential customers, including changes in demand, dissatisfaction, and loss of customers. Important to maintain loyalty, revenue recurrence, and brand reputation.

**Commercial:** Involves risks associated with commercial and market strategies, such as flaws in product and service design, marketing campaigns, inadequate pricing,



and changes in competition. Impacts the Company's revenue and position in the market.

**Accounting:** Refers to risks related to the accuracy of financial statements and compliance with accounting standards. It is relevant to avoid financial errors and maintain the confidence of investors, shareholders, and financial creditors.

**Development:** Risks associated with product or service development projects, such as innovation failures, delays, outdated technologies, and cost overruns. It helps to ensure the competitiveness and efficiency of the products and services offered by the Company.

**Stock:** Risks related to inventory management, such as excess, lack of products, or obsolescence. Essential for the continuity of operations, meeting customer demands, and optimizing costs.

**Financial:** Involves risks of a financial nature, such as exchange rate fluctuations, interest rates, customer default, liquidity of financial resources, and access to credit. Important to ensure the financial health and stability of the Company.

**Tax:** Risks related to tax compliance and changes in tax laws. Serves to avoid penalties, maintain compliance with tax obligations, and minimize the impact of accounting provisions.

**Suppliers:** Concerns risks related to dependence on and performance of suppliers, such as delivery failures, unsatisfactory quality, and logistical problems. Important for the continuity of the Company's production chain.

**Infrastructure:** Refers to risks associated with the maintenance and operation of facilities and equipment, such as structural failures and disasters. Essential for the Company's uninterrupted operation.

**Legal:** Includes legal risks, such as litigation, non-compliance with legislation, and regulatory changes. Serves to protect the Company from legal penalties, maintain its compliance, and minimize the impact of accounting provisions.

**Logistics:** Risks related to the movement and transportation of products, such as delays, loss, and route failures. Directly impacts the efficiency of the Company's production chain.

## Campinas

Rua Doutor Ricardo Benetton Martins, 1.000  
Parque II do Polo de Alta Tecnologia  
Campinas • SP • CEP 13.086-510

+55 19 2104-9700  
+55 19 2104-9703  
padtec@padtec.com.br

**Manufacturing:** Refers to risks in the production process, such as technical failures, waste, and inefficiency. Important to maintain the quality and efficiency of all stages of production.

**People:** Involves risks related to human resources management, such as high turnover, lack of training, and internal conflicts. Essential for retaining employees and maintaining the Company's productivity.

**Planning:** Risks related to strategic and operational planning, such as flawed projections and inadequate plans. Serves to ensure the execution of strategies aligned with the Company's objectives.

**Products:** Refers to risks associated with the quality, safety, and acceptance of products. Important for customer satisfaction and compliance with market standards.

**Quality:** Involves risks of failure to maintain quality standards in processes and products. Impacts the Company's production chain and maintaining customer loyalty.

**Services:** Refers to risks in the provision of services, such as failures in development, delivery, and customer service. Essential to maintain customer trust and satisfaction.

**Supplies:** Risks associated with the acquisition and management of raw materials and resources required for the Company's production chain. Serves to maintain efficiency and avoid interruptions in production.

**Technology:** Involves risks related to the use and implementation of new technologies, such as software failures and obsolescence. Important for the Company's innovation and competitiveness.

Thus, risk analysis involves developing an understanding of the risks mapped in Stage 2. Based on this understanding, Stage 4 of Risk Assessment is reached and decisions are made about which treatments to adopt, as well as which strategies and methods are most appropriate for their management.



## **Step 4: Risk Assessment**

The Risks mapped and analyzed are evaluated according to their potential materialization impacts to achieve the Company's objectives.

### **Campinas**

Rua Doutor Ricardo Benetton Martins, 1.000  
Parque II do Polo de Alta Tecnologia  
Campinas • SP • CEP 13.086-510

+55 19 2104-9700  
+55 19 2104-9703  
padtec@padtec.com.br

In this sense, the Company's Management, Risk Owners and process leaders jointly assess the Events from the perspective of Probability, Frequency and impacts. In the Risk assessment process, variables are sought to combine qualitative and quantitative methods. Thus, variables are considered, among others, for the classification of impacts that help in the better classification of Risks, using the high, medium and low gradient for each variable.

Finally, combining all the evaluation variables, the criticality of the identified Risks is defined, which allows the construction of a prioritization map, starting from the Risks with the highest exposure to those with the least exposure.

This map helps the Company to obtain a greater degree of alignment of strategic planning with its acceptable level of Risk Appetite.

In this sense, Step 4 is crucial in assisting the Company's Management in making decisions regarding the Risks that should or should not be prioritized.

In addition, a general assessment of the Company's Risks is carried out annually, led by the Board of Directors, with the participation of the Executive Board and the members of the Statutory Audit and Risks Committee, through meetings and interviews, whose objective is to carry out the diagnosis of the Company's structure, identify the Risks, define the prioritization in the treatment of the identified Risks, prepare a new Risk map, define the Risk management strategy and, consequently, the human and financial resources necessary to operationalize the Company's Risk Management structure.

However, despite the periodicity of the general assessment described above, the Risk map is subject to adjustments at any time (exclusion, modification and addition of Risks and priorities) if changes are observed in the reality of the Company that justify such adaptability.



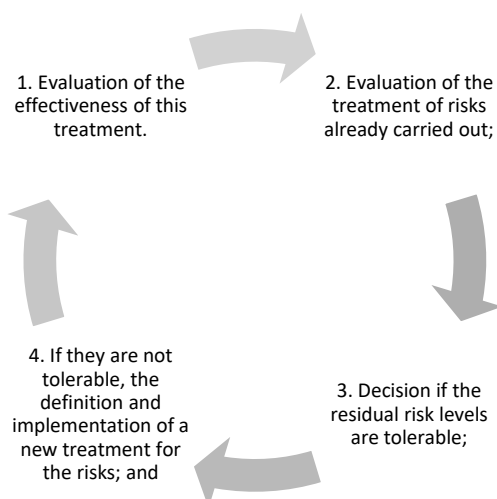
## **Step 5: Risk Treatment**

The Risk Treatment phase involves identifying the existing Control devices within the process for analyzing the effectiveness of these Controls as preventive measures and as factors that reduce the degree of exposure (Mitigating Factor), to arrive at Residual Risk.

For processes that require a greater degree of effectiveness of the Controls or that do not have effective mitigation factors, the Risk will be treated by the Risk

Management and Internal Controls area together with the area responsible for the 1st Line of Defense of this Risk, through the implementation of one or more Action Plans that aim to mitigate the exposure to the Risk and/or the impacts in the event of materialization of an Event associated with it.

For each Action Plan, those responsible and the implementation schedules are assigned to ensure the effectiveness and efficiency of the Plans and thus reduce the level of Residual Risk.



In this process, for each Risk Treatment action, a response to the Risk must be provided, which can be:

- Accept (nothing to do): do not take any action to reduce the Probability or the impact of the Risk. This alternative should be applied when the cost of management/mitigation does not compensate, if compared to the assumed impact, within the acceptable level of Risk Appetite defined by the Company. In this case, the Risk must be monitored continuously to guarantee a new appropriate treatment if there is a change in the situation that may increase the impact and/or probability of the Risk - generating a change in its criticality.
- Eliminate: adopt actions that alter or eliminate a process or a project, protecting the business objectives from the impacts of a given Risk.
- Mitigate (internal control): define internal controls to mitigate risks and/or reduce the probability of the Risk occurring and/or its impact in the event of occurrence. This alternative should be applied when the reduction in Probability or impact is sufficient to make the risk acceptable, according to the Company's Risk Appetite.

When opting for a specific action in the Risk Treatment process, the responsible executives and managers must analyze the cost benefit of the action, considering the costs involved, efforts and implementation, as well as studying the benefits resulting from the action in the financial, legal and reputational scope, among others. The treatment plan must identify the order of priority in which each Treatment should be implemented.

After determining together with the liable and/or affected areas the treatment strategies to be adopted, the Action Plan will be documented and communicated to the areas involved to ensure the timely implementation of the determined measures.

The Risk Management and Internal Controls area will support the areas in the preparation of Action Plans to correct the control failures identified in the root cause and mitigate the identified Risks.



## **Step 6: Monitoring**

The Company's monitoring processes are intended to ensure that Risk Controls are effective and efficient in their implementation, with the achievement of the intended results and strategies designed by Management and the Lines of Defense.

Through the monitoring process, it is possible to obtain information that can better guide the phases of Risk assessment, analysis of Events, changes, trends, successes and failures, detection of changes in the Internal and External Contexts, and identification of emerging Risks. The results of the monitoring must be recorded and reported to those responsible for Risk Management and Internal Controls areas in the Company.

In this scenario, the monitoring of Risks is constituted in a dynamic and continuous cycle, being fundamental to guarantee in a timely, preventive and reactive manner actions that help to minimize impacts in case of materialization of Risks.

Monitoring must be carried out by the 1st Line of Defense, seeking to continuously evaluate the effectiveness of its controls and the improvement in the management of its Risks. The Risk Management, Internal Controls, and Compliance area (2nd Line of Defense) will support the business areas in the monitoring of risks, to contribute to the achievement of the objectives and goals of the Company.

Thus, the employees involved in each area must have the capacity and competence to identify, assess, prioritize, monitor and manage the Risks of their responsibility,

considering all changes within the internal and external environment of the Company, so that they can obtain a higher degree of control of their processes and, consequently, so that they can achieve the objectives established during the Risk Management.

The monitoring process is also linked to the implementation of the Action Plans, which will be prepared and put into practice by the business units under the responsibilities and periodicity defined by the owners of the Risks and by the areas of Internal Audit and Risk Management and Controls Company's internal staff.

## **Prisma System - GRC**

The Prisma-GRC System contains a detailed description of all the Company's processes, including associated Risks, Internal Controls previously tested by the Internal Audit area, as well as Absences and Deficiencies in Controls identified and internal audits performed.

All Company employees have access to the Prisma-GRC System to consult the processes, Risks, and linked internal controls, which are meticulously documented on the platform.

The managers responsible for each specific area also have access to information regarding Absences and Deficiencies in internal controls, as well as records of internal Audits carried out.



## **Step 7: Communication**


Risks must be communicated clearly and objectively, with all relevant information possible, to all affected and/or responsible parties, and, mainly, to the parties responsible for determining and implementing measures for their treatment.

Likewise, once the measures to be adopted to deal with the Risks have been determined, they must be communicated in a precise and rapid manner to the areas responsible for implementing the determined measures.

### **Campinas**

Rua Doutor Ricardo Benetton Martins, 1.000  
Parque II do Polo de Alta Tecnologia  
Campinas • SP • CEP 13.086-510

+55 19 2104-9700  
+55 19 2104-9703  
padtec@padtec.com.br





## 8. Validity and Review of the Policy

This Policy was approved by the Company's Board of Directors at a meeting held on February 23, 2021, and amended at a meeting held on March 25, 2025. It must be reviewed whenever necessary and will remain in force for an indefinite period.

## 9. References

- ABNT NBR ISO 31.000 / 2009: Gestão de Riscos – Princípios e diretrizes.
- As três linhas de defesa no gerenciamento eficaz de riscos e controles, IAA (*The Institute of Internal Auditors*) 2013.
- Código de Ética e Conduta da Companhia.
- COSO – ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework*.
- Guia de Orientação para Gerenciamento de Riscos Corporativos IBGC (Instituto Brasileiro de Governança Corporativa) 2007.

### Campinas

Rua Doutor Ricardo Benetton Martins, 1.000  
Parque II do Polo de Alta Tecnologia  
Campinas • SP • CEP 13.086-510

+55 19 2104-9700  
+55 19 2104-9703  
padtec@padtec.com.br