Company's Corporate Risk Management Policy

The Corporate Risk Management Policy establishes the guidelines applicable to the business and to the set of processes and procedures regarding the identification, analysis, evaluation, prioritization and treatment of existing corporate risks, in order to guarantee the sustainability of the business and the creation of value to the shareholders.

This document presents the Corporate Risk Management process of **SER EDUCACIONAL S.A.** (Company)**,** describing the related concepts, the work methodology used, organizational structure and responsibilities.

This Policy applies to the entire Company and its Subsidiaries.

1. CONCEPTS

1.1. EVENTS

Incident or occurrence, from internal or external sources to an entity, capable of affecting the achievement of the Company's objectives.

1.2. RISKS

Threat of events or actions that may impact the achievement of the Company's objectives. It is inherent to any activity and can affect assets, people, results, liquidity, image or business continuity.

1.3. RISK DISPOSITION

Degree of exposure to risks that the Company's Management indicates as acceptable to achieve its objectives and create value to its shareholders, taking into account the impact and probability of events.

1.4. INHERENT RISK

Degree of risk that is presented to the organization in the absence of any management measure that could change the probability or impact of a risk.

1.5. RESIDUAL RISK

Degree of risk that remains after managers have implemented the action plan to reduce the likelihood or impact of the risk.

1.6. LIKELIHOOD

Possibility of occurrence of certain event.

1.7. IMPACT

Result of certain event.

1.8. STRATEGIC RISKS

Risks associated with the macroeconomic, political, regulatory and competition environments, as well as investment and acquisition decisions taken by senior management, which could generate a substantial loss in the Company's economic value.

1.9. OPERATIONAL RISKS

Risks associated with the possibility of losses resulting from failure, deficiency or inadequacy of any internal processes, involving people, assets, systems or any external events that may adversely impact the Company's operations.

1.10. FINANCIAL RISKS

Risks associated with the exposure of the organization's financial operations (market, credit and liquidity).

1.11. CYBERSECURITY RISKS

Information technology and operational risks associated with physical security and cybersecurity, availability of infrastructure and systems, and data privacy.

1.12. MAP OF CORPORATE RISKS

Result of the process to identify potential risk events, carried out by the Executive Board, which includes the assessment of the likelihood and impact of these risk events at the Company.

1.13. ACTION PLANS

Activities that must be performed by managers in order to mitigate the severity of risks.

2. METHODOLOGY

The risk management methodology used by the Company is based on COSO ERM, an international reference model in the Corporate Risk management structure.
This methodology emphasizes the importance of creating an environment that values the risk

management process, integrity and ethical values, considering the following steps:

2.1. Consideration of strategic objectives;
2.2. Identification of risk events;
2.3. Risk assessment;
2.4. Consolidation of the risk map
2.5. Action plan; and
2.6. Monitoring.

2.1. CONSIDERATION OF STRATEGIC OBJECTIVES

It comprises the consideration of strategic objectives as a basis for mapping risks: strategic, operational, financial and cybersecurity, as well as communication and compliance processes.

2.2. RISK EVENT IDENTIFICATION

It comprises the identification of potential risk events that, if any, will affect the organization and loss of value for its shareholders.

2.3. RISK ASSESSMENT

Risk assessment allows the organization to consider the extent to which potential events could impact the achievement of objectives. Managers assess events from two perspectives – likelihood and impact, and generally use a combination of qualitative and quantitative criteria.

Risk = Impact x Likelihood

The multiplications between the weights associated with the degrees of likelihood and impact define the levels of inherent risks.

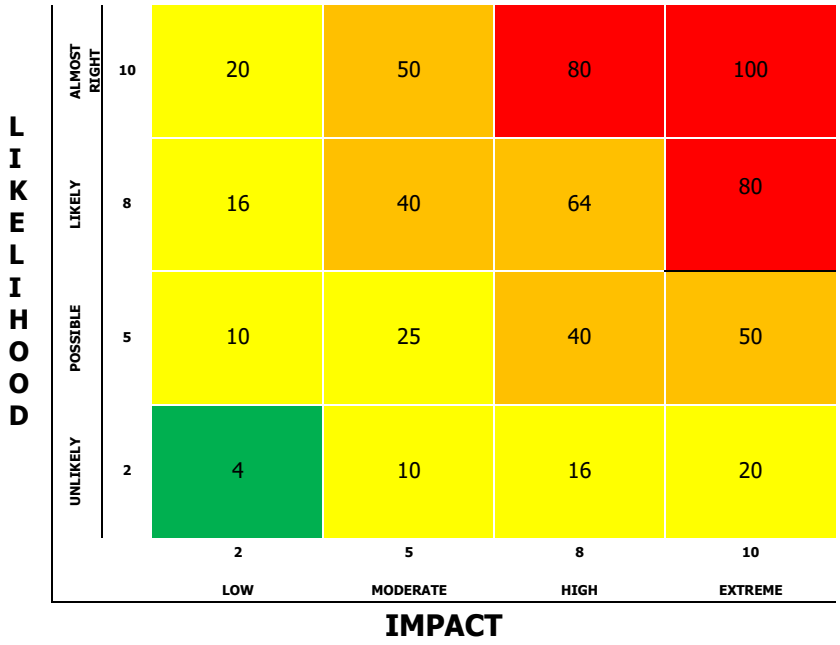
ASSESSMENT RULER

The Company established the following likelihood and impact criteria:

LIKELIHOOD		
Degree	**%**	**WEIGHT**
Almost right	>90%	10
Likely	>60% and <=90%	8
Possible	>30% and <=60%	5
Unlikely	<=30%	2

IMPACT						
Degree	Financial	Technology	People	Legal	Image	WEIGHT
Extreme	> R$ 50 MM	Unavailability of critical information and systems	Fatal accident	Suspension of unit operations with accountability of the legal representatives.	External Repercussion (National Media and Regulatory Agencies)	10
High	> R$ 10MM <= R$ 50MM	Leakage and/or loss of data and information	Accident with permanent disability	Shutdown of unit operations	External Repercussion (National Media)	8
Moderate	> R$ 1MM <= R$ 10MM	Handling of Information by Third Parties	Accident with temporary disability	Notification with enforcement of fines	External Repercussion (Regional Media)	5
Low	< R$ 1MM	Handling of Internal Information	Accident without damage	Notification without enforcement of fines	External Repercussion (Local Media)	2

The occurrence of an event can impact one or more dimensions (financial, technology, people, legal and/or image).



Graphic visualization of risk levels (RISK MAP)

2.4. CONSOLIDATION OF THE RISK MAP

The Risk Management Department is responsible for the methodology, annual consolidation and periodic monitoring of changes in the Company's Risk Map, based on assessments carried out by the Executive Board.

2.5. ACTION PLAN

After setting the Risk Map, the Executive Board will assess its responses to the risks, through action plans. Possible actions include:

- **Avoid:** discontinuance of the activities generating the risk.
- **Mitigate:** adoption of control(s) to reduce the likelihood and/or impact of risks.
- **Share:** reducing the likelihood and/or impact of risks by transferring or assigning a part of the risk.
- **Accept:** no measures are taken to mitigate the likelihood and/or impact of the risk.

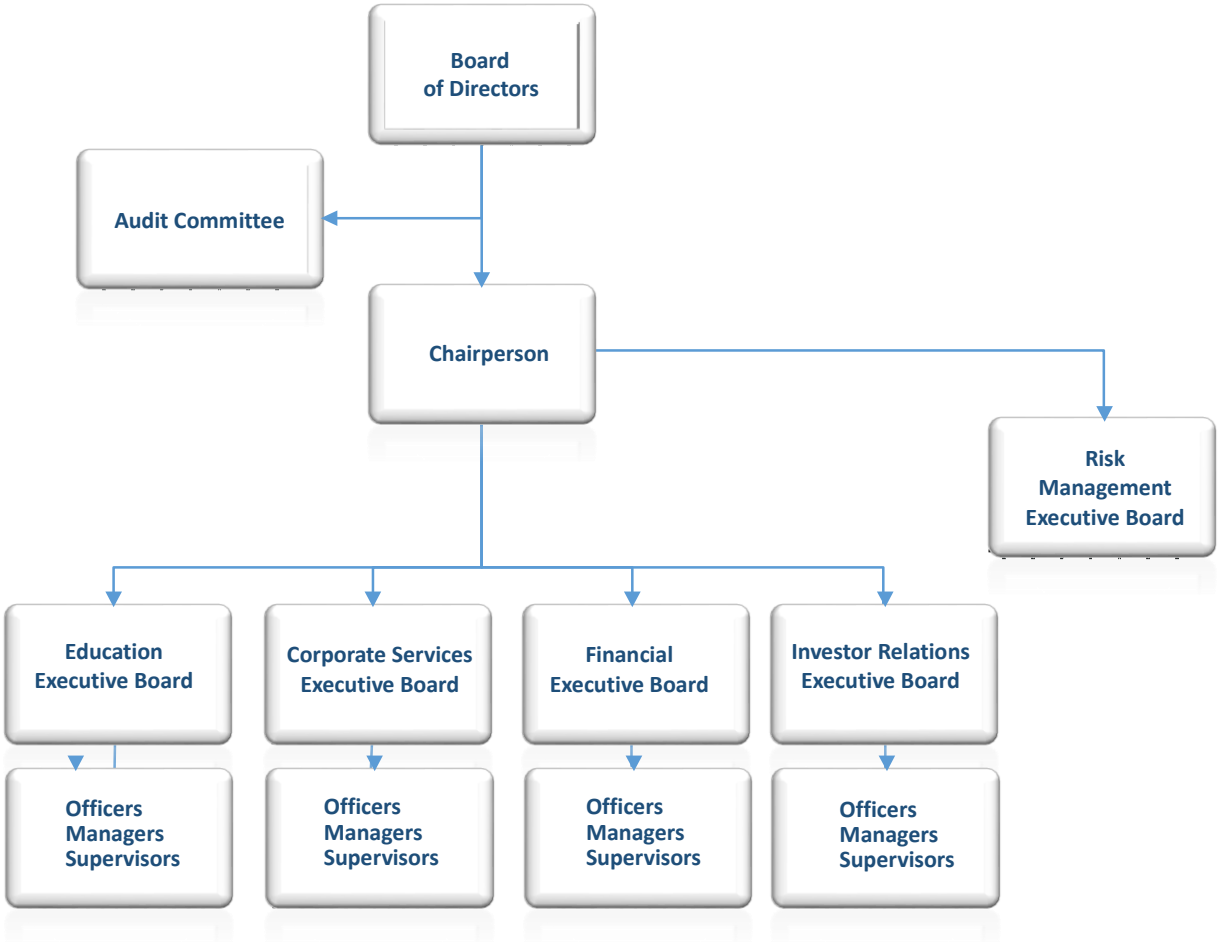
The action plans that are developed must be presented to the Risk Management Board within a maximum period of 60 days, indicating the owner of the risk, the person in charge for the execution, the schedule and, if necessary, the budget. The Risk Management Board will submit the action plans for approval by the President.

2.6. MONITORING

Monitoring must be carried out through continuous processes by the respective risk owners. Any deficiencies must be reported to the Risk Management Executive Board and the most serious issues reported to the Executive Board and the Audit Committee.

3. ORGANIZATIONAL STRUCTURE FOR RISK MANAGEMENT

The structure that performs the Company's Risk Management functions is represented in the following organization chart:



4. RESPONSIBILITIES IN RISK MANAGEMENT

4.1. RISK MANAGEMENT PROCESS

The risk management process must be continuously conducted by the Executive Officers and implemented by the other officers, managers and supervisors of the Company. The Risk Management area will assist the Executive Board in this implementation, based on the methodology described above. The Board of Directors, with the support of the Audit Committee, will be responsible for approving and reviewing the consolidated corporate Risk Map on an annual basis.

4.2. BOARD OF DIRECTORS

- Approve and review the Corporate Risk Management Policy;
- Provide strategic direction and support the Executive Board in the implementation of action plans and establish the management of consequences in the event of non-compliance with the guidelines; and
- Analyze and approve the Company's Risk Map.

4.3. CHAIRPERSON

- Continuously sponsor the Risk Management process;
- Analyze the Company's Risk Map, submitting it annually for approval by the Board of Directors.
- Promote the integration of the Risk Management process with the Company's planning, budget and management cycles; and
- Approve and ensure that action plans to avoid and/or mitigate identified risks are carried out in a timely manner.

4.4. EXECUTIVE BOARD

- Execute the Risk Management Policy and update, at least annually, the Risk Map of their respective areas, proposing any adjustments;
- Review and propose action plans to respond to the risks identified in your area and/or unit; and
- Continuously monitor the implementation of action plans defined for risk treatment.

4.5. OFFICERS, MANAGERS and SUPERVISORS

- Identify and manage the risks of their respective areas;
- Participate in the elaboration of action plans; and
- Implement defined action plans for risk treatment.

4.6. AUDIT COMMITTEE

- Advise the Board of Directors on its responsibilities in risk assessment and mitigation; and
- Support the Risk Department in the performance of its responsibilities.

4.7 RISK MANAGEMENT EXECUTIVE BOARD

- Disclose the Risk Management Policy and its methodology;
- Systematically monitor the Risk Management process in order to ensure its effectiveness and the fulfillment of its objectives;
- Ensure that the management areas carry out the identification, mapping and response

to risks, as well as the creation and implementation of controls over those risks;

- Prepare recommendations for the management areas and for the Executive Boards, in order to assist them in the control and procedure preparation or decision-making processes in order to mitigate the identified risks;
- Carry out follow-up of improvement actions related to risk mapping;
- Advise the Board of Directors, the Audit Committee, the President and other Executive Boards in matters related to risks;
- Annually reassess the adequacy of the Company's controls for risk management, reporting such analysis to the Audit Committee and/or Board of Directors; and
- Propose the updating of the Risk Management Policy, where deemed necessary.

4.8 INTERNAL AUDIT

- Prepare the planning and perform audit tests of the action plans and internal controls performed by the management areas (1st Line) and by the support areas (2nd Line); and
- Timely report the results of the controls tests to the Audit Committee and Risk Management Board, as well as new risks and controls identified for each project.

4.9 THREE DEFENSE LINES MODEL

The Three Defense Lines model is a simple and effective way to improve communication in risk management and expand the culture of risk mitigation by clarifying essential roles and responsibilities.

The significant points in this model are the objectivity and transparency about the responsibilities of each one in the conduct of business, operation and risk management in the Company.

In summary:

- The **1st Defense Line** is comprised of officers, managers and supervisors who are responsible for identifying and managing the risks in their areas;

- The **2nd Defense Line** is comprised of professionals whose objective is to support the 1st Line, by providing knowledge and adequate tools for them to fulfill their responsibilities. This line includes specialists in processes, quality, internal controls, risk management, controllership, compliance, among others; and

- The **3rd Defense Line** is summarized in the internal audit activity, which aims at an objective and independent assessment of the organization's risk management, controls and governance. The result is the communication of identified gaps and suggestions for improvements.

Approved by the Board of Directors on May 24, 2022