Wilson, Sons

INTEGRATED RISK MANAGEMENT POLICY OF WILSON SONS S.A.

August 7, 2024

ENGAGE WITH US:


wilsonsons.com.br/ir


Instagram.com/WilsonSons


Twitter.com/WilsonSonsBR


YouTube.com/WilsonSonsIR

INDEX

INTEGRATED RISK MANAGEMENT
POLICY OF WILSON SONS S.A.

1. INTRODUCTION

1.1. We hereby establish the Integrated Risk Management Policy of Wilson Sons S.A. ("Wilson Sons" or "Company"), expressing our commitment to maintaining the organization's longevity and, consequently, meeting the strategic and statutory objectives.

2. APPROVAL

2.1. This Policy has been approved in a meeting of the Board of Directors of the Company held on August 7, 2024, under the terms of article 13, item (w) of the Company's articles of incorporation.

2.2. The Board of Directors of the Company is exclusively responsible for approving any changes to this Policy.

3. PURPOSE

3.1. The scope of the Integrated Risk Management Policy defines a set of concepts, guidelines and responsibilities to ensure the excellence of Wilson Sons Integrated Risk Management. This set has the purpose of ensuring that potential adverse impacts and opportunities are formally managed, incorporating the vision of risks to strategic decision making, in accordance with the best market practices.

4. SCOPE

4.1. The Company and all of its subsidiaries, through the business and support units, which directly or indirectly participate in the Integrated Risk Management process.

5. PRINCIPLES

5.1. As described in the main methods, the integrated risk management encompasses the following principles:

5.2. Risk management creates and protects value: the risk management contributes to the demonstrable achievement of objectives and to the improvement of performance regarding, for example, the safety and health of people, legal and regulatory compliance, public acceptance, protection of the environment, efficiency in operations, governance and reputation.

5.3. Risk management is an integral part of all organizational processes: risk management is not an activity held separately from the main activities and processes of the organization. Risk management is part of management's responsibilities and an integral part of all organizational processes.

5.4. Risk management is part of decision making: risk management assists decision makers in making conscious choices, prioritizing actions and distinguishing between alternative forms of action.

5.5. Risk management explicitly addresses uncertainty: risk management explicitly takes into account uncertainty, the nature of said uncertainty, and how it can be addressed.

5.6. Risk management is systematic, structured and timely: a systematic, timely and structured approach to risk management contributes to efficiency and consistent, comparable and reliable results.

5.7. Risk management is based on the best information available: the inputs to the risk management process are based on sources of information, such as historical data, experiences, feedback from stakeholders, observations, forecasts, and expert opinions.

5.8. Risk management is tailor-made: risk management is aligned with the organization's internal and external context and risk appetite.

5.9. Risk management is transparent and inclusive: the appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the organization ensure that risk management remains relevant and up- to-date. Involvement also allows stakeholders to be properly represented and to have their opinions taken into account when determining risk criteria.

5.10. Risk management is dynamic, interactive and capable of reacting to changes: risk management continuously perceives and reacts to changes. As external and internal events take place, the context and knowledge change, monitoring and critical risk analysis are carried out, new risks arise, some change and others disappear.

5.11. Risk management facilitates the continuous improvement of the organization: organizations should develop and implement strategies to improve their risk management maturity along with all other aspects of their organization.

6. APPROACH

6.1. The Company uses a methodological approach composed of 5 stages that make up the integrated risk management process:

(a) Identify and Categorize;

(b) Assess and Measure;

(c) Prioritize and Assign Persons in charge;

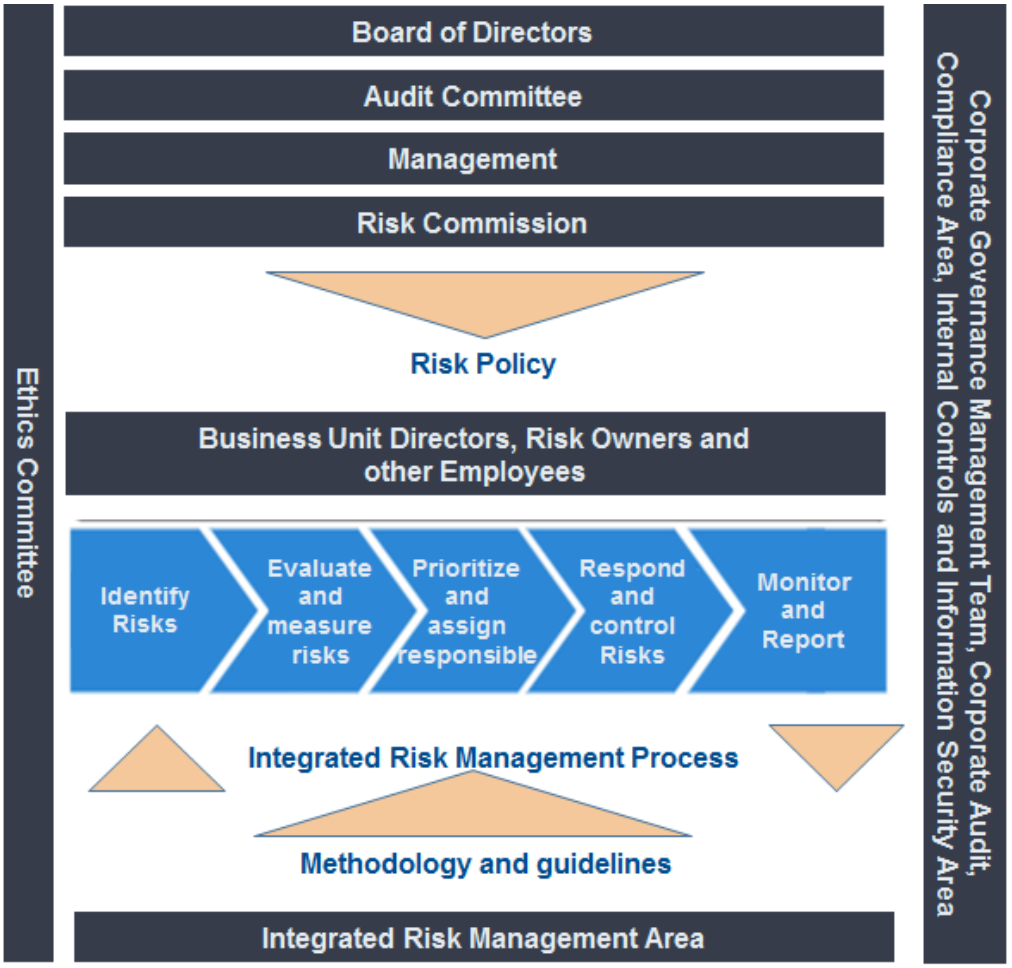
(d) Respond and Control Risks; and

(e) Monitor and Report.

6.2. The methodological process adopted uses the elements provided for in the Enterprise Risk Management (ERM) framework of the Sponsoring Organizations of the Treadway Commission (COSO) as a reference.

7. GUIDELINES

7.1. The Company identifies and addresses corporate risks in an integrated manner, in order to ensure compliance with the goals established in its strategic planning and good Corporate Governance practices. The guidelines define the Integrated Risk Management methodology processes and the governance applied for its proper functioning is composed of the following structure and components. For further details on such structures and components, see item 15 of this Policy.



7.2. This structure allows for synergy between the Senior Management and the various business units, in order to enable the adequate monitoring of the risks associated with the Company's operations.

8. RISK IDENTIFICATION

8.1. It consists of the search, recognition and description of risks by identifying the sources of risk, events, their causes and their potential consequences. Its purpose is to generate a comprehensive list of risks based on events that may prevent, reduce, accelerate or delay the achievement of strategic objectives.

8.2. The risk identification methodology must be defined and formalized by the risk management area. Please note that the process of identifying and analyzing risks in general must be monitored and continuously improved.

9. RISK CATEGORIZATION

9.1. The Company's Risk Dictionary defines a common language to be adopted by all agents involved in the process by segmenting risks into categories, as follows:

(a) Strategic Risks: Risks that may prevent or affect the achievement of the Company's strategic objectives;

(b) Financial Risks: Risks that may imply financial losses, resulting from unexpected effects on the economic scenario and market trends, reflected in the behaviour of interest rates, availability of credit, exchange rates, inflation, indebtedness, choice of financial investments, stock prices, among others;

(c) Operational Risks: Risks that may result in financial losses and image damage, resulting from operational deviations related to internal controls, processes, information systems, resource management, fraud, among others;

(d) Compliance Risks: Risks related to legal or regulatory sanctions, financial or reputation loss that the Company may suffer as a result of failure to comply with the application of laws (including the Brazilian Anti-Corruption Act - Law 12.846), regulations, ethics and conduct and internal policies;

(e) Technology Risks: risks related to instability and / or unavailability of the Company's technology environment (systems and assets) as well as the management of its accesses, which may result in interruption of operations, leakage of information and / or financial losses;

(f) Social and environmental risks: Risks related to events to which the Company is exposed and which may result in negative social and environmental impacts, as a

result of failure to comply with processes, regulations and requirements.

(g) Climate Risks: Risks related to the interference of climate change in the Company's business, divided into two categories: physical climate risks, referring to possible direct or indirect damage to the operations of the Company's Units, caused by acute or chronic events such as windstorms, storms and/or sea level rise; and transition climate risks that may affect the Company's performance, referring to regulatory, technological, reputational and/or market changes; and

(h) Emerging Risks: These are the risks with medium and long term impact, potentially relevant for the business, whose elements are not yet sufficiently known for their assessment, due to the number of factors and impacts that have not been fully assessed.

10. RISK ASSESSMENT AND MEASUREMENT

10.1. These are the processes to understand the causes, context, characteristics, potential impacts, probability of occurrence, speed and level of exposure to risks, in order to allow a more adequate response to them. Obtaining the information required by this process, including assigning the levels of probability of occurrence and impact of risks, should take place according to standards and metrics defined by the Integrated Risk Management Area.

10.2. The Company’s risks will be assessed in terms of probability and impact, and after qualitative and quantitative analysis, they will be prioritized considering the level of existing controls, thus ascertaining the residual risks.

10.3. Risks with financial impacts must have their calculation memory validated by the FP&A area.

10.4. It is worth noting that the probability dimension was created with the sole purpose of supporting the Company’s integrated risk management process, and acting as an internal support tool for the area with no relation to accounting criteria for financial statement purposes in general, including provisions and contingencies.

10.5. The detailed assessment criteria of impact and probability, as well as criteria for assigning responsibilities (Risk Owners) are covered in Annexes 2, 3 and 1 respectively.

11. RISK RESPONSE

11.1. Risk response is the process of developing strategic options and defining actions to increase opportunities and reduce threats to the entity’s objectives. Risk responses fall into the following categories:

(a) Avoid - Discontinuation of activities that generate risks. Avoiding risks may imply discontinuing an activity, operation or selling a division.

(b) Reduce - Measures are taken to reduce the probability and / or the impact of risks, mitigating their consequences for the Company.

(c) Share - Reduce the probability and / or impact of risks by transferring or sharing a portion of risk. Common techniques include purchasing insurance products, carrying out hedging transactions or outsourcing an activity.

(d) Accept - No measure can be taken to affect the probability or the degree of impact of the risks, or it is not in the interest of the Company to do so, leaving the monitoring and management of the exposure.

11.2. The Company has the following instruments to mitigate its main risks:

(a) Strategic Risks: throughout the year, the Company holds internal forums for discussions with its main executives about its strategic planning. To support the execution of the strategy, the Company has a profit sharing program with remuneration linked to performance in meeting targets (departmental and individual) directly linked to the execution of its strategy. There are also monthly results assessment meetings where performance indicators related to the goals are discussed and action plans are defined to correct the course of operations towards achieving the goals;

(b) Financial Risks: The Financial Department constantly monitors the national and global financial scenario and produces periodic reports assessing these scenarios and signaling any impacts on the smooth running of the Company's operations, as a strategy to mitigate these possible risks and support for making strategic decisions on the finance agenda. In addition, the Company may count on the support of external economic consultants for such assessments. Market risk management is carried out through systematic assessment of the risk position of the Company and its subsidiaries, taking into account current market conditions and budget projections for results and investments, in order to ensure liquidity, profitability and predictability, the following assessments being carried out: (a) liquidity projections for two fiscal years; (ii) stress tests varying currency parities and impacts on results and cash flows; (iii) monitoring of cash generation by currency; and (iv) evaluation of balance sheet currency exposures. Additionally, for purposes of asset protection (hedge), in general, for operating cash flows, an attempt is made to offset the currency risk by matching revenues and costs, as well as assets (receivables) with liabilities (payments) in R$. The goal is to have the net cash generation in US dollars. Cash flows from investments in fixed assets are also denominated in different currencies and are monitored with the objective of matching the terms and currencies of the sources of funds. The following financial instruments are used for equity protection (hedge): (i) with cash: (a) foreign exchange investment funds; (b) CDBs with US dollar swap; (c) government exchange bonds and (d) export notes; and (ii) without cash: (a) swap contracts; (b) currency forward contracts; and (c) purchase of option contracts;

(c) Operational Risks: the Company has an internal controls area that tests internal controls during the year to ensure its efficiency and effectiveness. The functions of this area include judging whether the way in which the internal controls were designed is sufficient to mitigate operational risks to a level acceptable to the Company. When weaknesses in internal controls are identified, the area recommends improvements that are evaluated and implemented by process managers. In addition, there is monthly monitoring of performance indicators for organizational processes in monthly result meetings. For indicators with unsatisfactory performance, action plans are created to correct the identified situations;

(d) Compliance Risks: the Legal Department maintains continuous monitoring of compliance with laws and regulations to which the Company is subject. The Institutional Communication Department continuously monitors any situations, facts, news that may affect the Company's operations or image. The Compliance Department performs continuous management and monitoring of the Integrity Program, aiming to enhance the control environment and initiatives for training and acculturation regarding ethical and anti-corruption precepts;

(e) Technology Risks: to reinforce the security of its technology infrastructure and information systems, the Company periodically reviews the internal controls related to IT in order to increase the security of the information systems by improving internal controls;

(f) Social and Environmental Risks: continuous monitoring by the HSE Department of the potential or actual effects generated by the Company's activities on the environment and society. If (potential or actual) negative impacts are identified, the HSE Department shares such facts to the Company's management in order to define an action plan, if necessary;

(g) Climate Risk: The Company has incorporated the TCFD (Task Force on Climate-Related Financial Disclosures) approach to its management of risks and opportunities related to climate change (further details available in the Sustainability Report). The Company has been conducting an inventory of its greenhouse gas emissions since 2013 and has several initiatives aimed at reducing its carbon intensity. Meteorological data, oceanographic and tidal data are monitored to ensure infrastructure and operational safety. Currently, Wilson Sons monitors the market movements and the impacts suffered by its customers with a dedicated market intelligence team. Moreover, the Company is always looking for ways to diversify its activities and seek opportunities that such market changes may bring; and

(h) Emerging Risks: Controls and mitigation measures for emerging risks are addressed according to the nature of the risk, such as, for example, climate risk management measures or the COVID-19 pandemic.

12. RISK CONTROL AND MONITORING

12.1. The Integrated Risk Management area must monitor the existence of controls, the performance of risk indicators as well as their limits and oversee the implementation and maintenance of action plans through continuous management and / or independent evaluations, with the assistance of Internal Controls for the assessment, adequacy and testing of controls for eligible risks by Governance and Integrated Risk Management.

12.2. Risk owners must carry out regular and timely assessments of the risks under their responsibility, considering at least an annual assessment, with support from the Integrated Risk Management area.

13. RISK COMMUNICATION AND REPORTING

13.1. Communication during all stages of the integrated risk management process must reach all stakeholders and be carried out in a clear and objective manner, respecting good governance practices.

13.2. The communication seeks to ensure a timely flow of relevant information related to risks at the various hierarchical levels of the Company, including the processes of identification, assessment, analysis and response to risks. This process must be able to demonstrate, in a timely, clear and frequent manner, what are the main risks to which the Company is exposed, as well as what are the existing and / or planned actions to respond to these risks, so as not to compromise the defined business strategy.

14. EXPOSURE LIMITS

14.1. The limits of exposure and tolerance to risks are validated by the Board of Directors, on its own initiative or as proposed by the Executive Board or the Audit Committee. These are associated with the level of exposure to risks to which the Company is willing to accept in order to achieve its strategic goals and create value for the shareholders.

14.2. The Company's risk appetite is validated by the Board of Directors, on its own initiative or upon proposal of the Executive Board or the Audit Committee. Its formalization and safeguarding are the responsibility of the Risk Commission.

15. ROLES AND RESPONSIBILITIES

Area/Responsible	Responsibility
Board of Directors	I. Validate, on its own initiative or whenever proposed by the Executive Board or the Audit Committee, the strategic issues of Integrated Risk Management, such as the degree of risk appetite of the Company and its tolerance ranges; II. Ensure operational autonomy to the Audit Committee, approving its own budget, intended to cover operating expenses; III. Assess, at least annually, whether the structure and budget of the internal audit are sufficient to perform its functions; IV. Approve this Policy and its revisions.
Executive Board	I. Clearly define the risk appetite and define guidelines, resources and goals that ensure the proper functioning of integrated risk management (without prejudice to the specific attributions of the Chief Financial Officer and the Chief Operating Officer, in their respective scopes, as described below), to be validated by the Board of Directors, pursuant to this Policy, observing the Integrated Risk Management guidelines established by the Board of Directors; II. The Chief Financial Officer has specific duties to lead the administration and management of the financial activities of the Company and its subsidiaries, including the analysis of investments and definition of risk exposure limits, proposal and contracting of loans and financing, treasury operations and the planning and financial control of the Company; III. The Chief Operating Officer has specific duties to lead the administration and management of the operations of the Company's subsidiaries, including the definition of operating strategies and operating risk exposure limits.
Risk Commission	I. Assess the strategies and models applied in the Integrated Risk Management, the portfolio and relevant risk assessments; periodically assess, monitor and reassess the risks to which the Company is exposed; prioritize resources for risk response; report risks to the various stakeholders; monitor the execution of this Policy and compliance with the standards related to Integrated Risk Management. II. The Risk Commission reports to the Executive Board, being composed of Executive Officers (Chief Executive Officer, Chief Financial Officer and Chief Operating Officer), Non-statutory Officers (Legal Officer, Institutional Relations Officer, Human Resources Officer, Information Technology Officer, Strategy and New Business Officer, and Governance Officer); in order to, when requested, provide information to the Board of Directors on matters related to its scope.
Audit Committee	I. Validate the Company's risk exposure and tolerance limits; II. Validate, whenever proposed by the Executive Board or on its own initiative, strategic issues of Integrated Risk Management, such as the degree of risk appetite of the Company and its tolerance ranges; III. Monitor the activities of the Company's internal audit and internal controls area; IV. Assess and monitor the Company's risk exposures; V. Evaluate, monitor, and recommend to management the correction or improvement of the Company's internal policies, including the Related Party Policy.

Area/Responsible	Responsibility
	VI. Receive information and assess non-compliance with legal and normative provisions applicable to the Company, in addition to internal regulations and codes, including provision for specific procedures to protect the provider and the confidentiality of information. VII. The Audit Committee is directly linked to the Company's Board of Directors.
Non-statutory Officers and other employees	I. As part of the first line of defense (as well as the Risk Owner), they are responsible for the adequate and efficient maintenance of the risk matrix, which includes the validation and prioritization of the business unit's risks and their response measures, in line with this Policy.
Risk Owners	I. As part of the first line of defense (as well as the Non-statutory Officers and other employees), they are responsible for identifying, assessing,responding, monitoring and reporting risks, implementing and reporting action plans and controls, involved in the operations under its management, in accordance with the resolutions taken together with the Integrated Risk Management Area, Corporate Audit, the Risk Commission and Senior Management (Executive Board and Board of Directors).
Governance Department	I. As part of the second line of defense, it is responsible for (i) carrying out the technical analysis of transactions with related parties, pursuant to the Related Party Transaction Policy, in addition to the Audit Committee; (ii) submit the requested transactions for the approval of the Executive Board; (iii) properly file forms, and manage the information contained therein, pursuant to the Related Party Transaction Policy; and (iv) provide guidance and clarification to the entire Company. II. The Governance Department reports to the Chief Executive Officer, through the Governance Director, and comprises the following areas: (i) Integrated Risk Management, (ii) Internal Controls, (iii) Compliance and (iv) Information Security Audit, which are detailed in the following items. III. The members of the Governance Department do not accumulate operational activities in the Company.
Integrated Risk Management	I. As part of the second line of defense, it is responsible to provide methodologies and tools for the Integrated Risk Management; supervise the goals, mitigation actions and risk treatment and ensure that the risk owners implement the necessary actions to establish the control environment and to help in the treatment of identified risks; as well as disseminating the risk culture in the Company. It supports the identification, assessment, treatment and reporting of existing risks, associated controls and mitigation action plans. II. As described above, the Integrated Risk Management Area is an area of the Governance Department. III. Members of the Integrated Risk Management Area do not accumulate operational activities in the Company.
Internal Controls	I. As part of the second line of defense, it controls the validity period and review of this normative document and, whenever necessary, supports the review process together with the area that manages the process. II. Test established controls. III. As described above, the Internal Control Area is an area of the Governance

Area/Responsible	Responsibility
	Department. IV. Members of Internal Controls do not accumulate operational activities in the Company.
Compliance	I. As part of the second line of defense, it is responsible for (i) carrying out the compliance program, aimed to disseminate the Company's ethical and anti-corruption culture, whose initiatives include training; Employees so that ethical and anti-corruption concepts are renewed; (ii) For the preparation, management, application, oversight, communication, and updating of the Code of Ethical Conduct, as well as determining necessary actions for the dissemination and promotion of the highest standards of ethical conduct within the Company; (iii) report its activities to the Company's Executive Board; and (iv) propose to the Executive Board actions that contribute to consolidate the culture of ethics/anti-corruption with the Company stakeholders. II. The members of the Compliance Area do not accumulate operational activities in the Company.
Information Security Audit	I. As part of the second line of defense, it is responsible to check and confirm the confidentiality, accessibility, integrity, availability and authenticity of information from corporate systems connected to the businesses, and potential implications to them, in the event of any Information Security incidents. II. As described above, the Information Security Audit is an area of the Governance Department. III. Members of the Governance Department do not accumulate operational activities in the Company.
Internal Audit	I. As part of the third line of defense, it is responsible for assessing and supervising the adherence and effectiveness of the risk management process at the Company. The Internal Audit area acts independently and objectively, reporting functionally to the CEO and, when necessary, to the Audit Committee and Board of Directors.
Ethics Committee	I. As part of the second line of defense, it is responsible (i) for managing the Ethics Channel, dealing with reports and complaints received, pursuant to the Code of Ethical Conduct and Internal Regulation of the Ethics Committee; (ii) for carrying out an assessment on the acceptance of certain offers and offerings that may generate a conflict of interest by the Company's employees, pursuant to the Code of Ethical Conduct. II. The Ethics Committee is directly linked to the Company's Board of Directors. reporting its activities to the Board of Directors and functionally to the Chief Executive Officer. III. The members of the Ethics Committee do not accumulate operational activities in the Company.

16. GLOSSARY

- **Risk:** Possibility of something happening and having a negative or positive impact on the objectives, being measured in terms of consequences and probabilities.

- **Integrated Risk Management:** a process under responsibility of the entire organization - Board of Directors, Executive Board, Audit Committee and other employees - applied in the establishment of strategies created to identify potential events, capable of affecting it and to manage risks in order to keep them compatible with the organization's risk appetite and provide reasonable assurance of the achievement of its objectives.
- **Causes or Risk Factors:** Conditions that make possible the realization of an event that affects the objectives. They are the result of combining the sources of risk with vulnerabilities.
- **Event:** An event is an incident or occurrence that affects the implementation of strategy or the achievement of objectives.
- **Risk Source:** Element (people, processes, systems, organizational structure, physical infrastructure, technology, external events) that, individually or in a combined manner, has the intrinsic potential to give rise to risk. The risk sources include: threats and opportunities.
- **Residual Risk:** The risk that remains after management has taken steps to change the likelihood and / or the impact of the risks.
- **Impact:** Result or effect of an event. There may be a number of possible impacts associated with an event. The impact of an event can be positive or negative in relation to a company's related objectives.
- **Probability:** The possibility of occurring a given event;
- **Risk Appetite:** The amount or limit of exposure to risks that a company is willing to accept in pursuit of its mission (or vision).
- **Risk Tolerance:** The acceptable variation relative to the achievement of an objective.
- **Risk Owner:** Person or entity that has been given the authority to manage a specific risk and is responsible for doing so.
- **Priority Risks:** Group of risks with potentially high impact for the business unit, whose management must be prioritized and its indicators must be monitored regularly.
- **Key Risk Indicators (KRIs):** Main risk indicators of the Company. They function as warning signs, indicating changes in the risk level of an organization or its business units, and are fundamental components of a control structure and good risk management practices.

17. ANNEXES

- **Annex 1 -** Responsibilities for Risks (Risk Owners)
- **Annex 2 -** Impact

- **Annex 3 -** Probability

18. REFERENCES

- COSO Corporate Risk Management - Integrated Structure;
- ABNT NBR ISO 31.000:2009 - Risk Management - Principles and Guidelines;
- ABNT NBR ISO/IEC 31.010 - Risk management Techniques for risk assessment process.

19. DISCIPLINARY SANCTIONS

19.1. Non-compliance with this normative document is subject to disciplinary sanctions. Possible disciplinary measures include:

(a) Verbal warning;

(b) Written warning;

(c) Suspension; and

(d) Dismissal with or without cause.

19.2. Sanctions must be fair, reasonable and proportionate to the fault committed.

20. FINAL PROVISIONS

20.1. This Policy will be disclosed by the Company on the page on the Company's worldwide computer network (https://ri.wilsonsons.com.br).

20.2. This Policy will only come into force and its terms and conditions will become effective as of the date of entry into force of the Novo Mercado Participation Agreement, to be entered into between the Company and B3 S.A. - Brasil, Bolsa, Balcão and will remain in force for an indefinite period.

20.3. In the event of a conflict between the provisions of this Policy and the Company's articles of incorporation, laws or other applicable rules, the latter shall prevail.

20.4. Omitted cases will be decided by the Board of Directors of the Company.