
RISK MANAGEMENT POLICY

UNICASA INDÚSTRIA DE MÓVEIS S.A.

Approved at the Board of
Directors Meeting held on May 30,
2025.

CONTENTS

1. PURPOSE	3
2. SCOPE.....	3
3. CONCEPTS.....	4
4. THE RISK MANAGEMENT PROCESS.....	5
4.1 Analyzing context, establishing evaluation criteria, and defining risk appetite	6
4.2 Identify, map, and classify the risks	6
4.3 Evaluating and Prioritizing Risks	8
4.4 Responding to Riskst	9
4.5 Monitoring Risks and Internal Controls.....	10
4.6 Communicate.....	10
5. RESPONSIBILITIES.....	10
6. GENERAL PROVISIONS.....	14

UNICASA INDÚSTRIA DE MÓVEIS S.A.

RISK MANAGEMENT POLICY

1. PURPOSE

This Risk Management Policy establishes the principles, guidelines and responsibilities in managing the risks of Unicasa Indústria de Móveis S.A. and its subsidiaries (“Company”) so as to identify and monitor the risks related to the Company or its industry.

In this context, the purpose of the Company’s Risk Management is to control its activities and financial, operational and managerial information systems in order to ensure that:

- The business risks inherent to the Company’s activities are identified, assessed and mitigated to an acceptable level;
- The internal control framework is continuously reviewed, taking into account the risks existing in the business processes;
- Potential conflicts of interest are identified and associated risks are minimized;
- All employees clearly understand the objectives of the risk management process and the roles, functions and responsibilities assigned at different levels of the Company;
- Employees clearly understand their role, objectives, functions and responsibilities within the control functions established by the Company;
- Recommendations from users are properly implemented, in order to minimize the risk of the Company’s procedures being non-compliant with applicable laws and regulations (both internal and external); and
- The strategic objectives of the Company are fully achieved.

2. SCOPE

This Policy applies to the Company and its subsidiaries, as well as all employees, managers, statutory and non-statutory officers, members of the Board of Directors, committees and Audit Board (if applicable), representatives and third parties directly or indirectly related to the Company and its subsidiaries.

3. CONCEPTS

For the purposes of this Policy, the following concepts will be used:

- **Risk:** The possibility of an event that adversely affects the achievement of the Company's objectives or its processes.
- **Risk appetite:** Refers to the level of risk the Company is willing to accept in pursuing and achieving its strategy.
- **Priority risks:** Risks with potentially high probability and impact for the business, whose management must be prioritized and whose indicators must be monitored regularly.
- **Risk matrix/model:** Establishes an individual comparison of Risks based on the degrees of impact and probability of risk occurrence for the purpose of prioritization and management. The risk matrix is a constantly evolving mechanism that is updated at least annually when the Company's strategic plan is reviewed and promptly when Risk events arise.
- **Internal controls:** Process(es) or mechanism(s) created to provide reasonable assurance of achieving the Company's objectives by mitigating the inherent business risks, including, but not limited to, the establishment of the Company's internal oversight bodies (e.g., Audit Committee).
- **Three Lines Model:** Developed by The Institute of Internal Auditors (IIA), this model outlines the three primary roles involved in organizational risk management, formerly known as the Three Lines of Defense.
 - i. The First Line consists of the majority of the Company's employees, who are directly involved in operational activities and in delivering value to customers (e.g., sales, logistics, production, and procurement), including support functions (such as Human Resources, Information Technology, and Finance). In this context, process users and managers are directly responsible for identifying risks and implementing internal controls within their areas of responsibility, thus forming the frontline of corporate risk management.
 - ii. The Second Line represents specialized risk management functions that provide expertise, establish processes, and develop monitoring and oversight tools to support and advise the First Line. These include Risk Management, Internal Controls, Compliance, Quality, Occupational Health and Safety, Information Security, and Sustainability.
 - iii. The Third Line is responsible for verifying the effectiveness and quality of the Company's corporate risk management, internal controls, and governance processes, and is represented by the internal audit function.

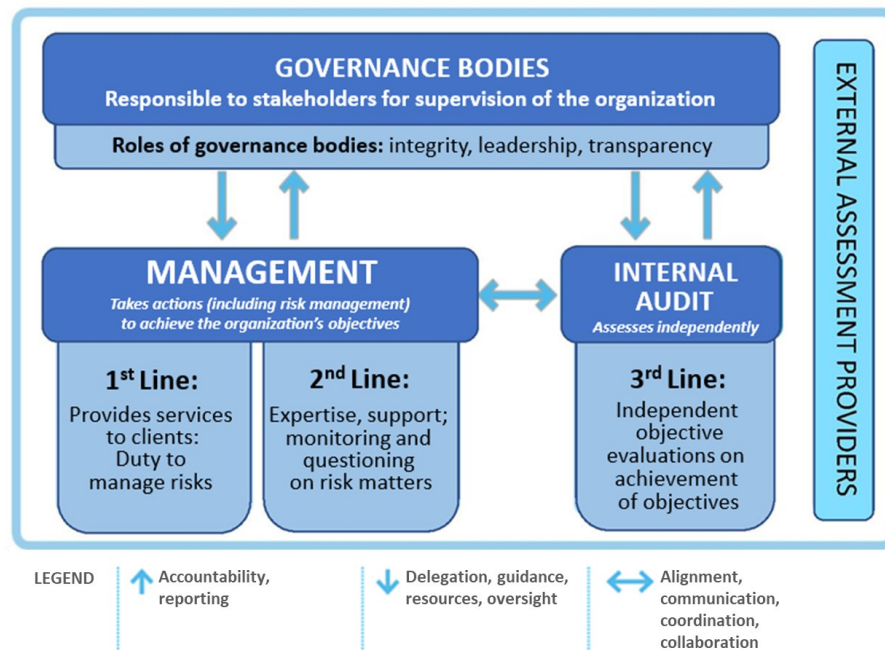


Figura 1: The IAA Three Lines Model

4. THE RISK MANAGEMENT PROCESS

The organizational structure of the Company's risk management processes uses as a parameter the guidelines established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), especially in relation to the flow of identification, evaluation, treatment, and monitoring of the risks to which the Company and its subsidiaries are exposed.

Thus, the process of risk management involves alignment between the objectives set and the Company's purpose, values, and strategic pillars, and it permeates all Unicasa business processes, since every activity carries some inherent risk.

To this end, the process is composed of six stages:

- (i) Analyze the context, establish evaluation criteria, and define the risk appetite;
- (ii) Identify, map, and classify the risks;
- (iii) Evaluate and prioritize the risks;
- (iv) Respond to the risks;
- (v) Monitoring risks and Internal Controls; and
- (vi) Communicate.

4.1 Analyzing context, establishing evaluation criteria, and defining risk appetite

This stage consists of understanding the Company's business environment and strategy, as well as evaluating how risks are perceived internally, how they are controlled, and how employees are guided in pursuing effective risk treatment. To this end, the Company seeks to understand the environment in which it operates, taking into account its values, culture, decision-making processes, operating style, and organizational structure. This stage also involves reviewing and assessing the main internal policies and manuals in order to understand how Unicasa documents its key processes and activities.

Based on this understanding of context, the Company establishes the criteria for risk evaluation. At this point, the Company also defines its risk appetite, which—aligned with the overall strategy—sets the business's exposure limits and serves as a reference for assessing and responding to organizational risks.

With support from the Audit Committee, the Board of Directors periodically analyzes and reviews Unicasa's risk appetite (acceptable level of risk).

4.2 Identify, map, and classify the risks

Understanding business processes is fundamental to effective risk management and consists of:

- (i) mapping the activities involved in the process;
- (ii) understanding, identifying, classifying, and recording—based on the previously defined evaluation criteria—the risks inherent to Unicasa's activities, present across various organizational processes.

This process should consider historical risk materialization assessments, derived from various sources (e.g., audits, ethics hotline, and other records), as well as changes in the business context.

Risk identification and classification should be conducted by the Internal Controls, Risk and Compliance area (Second Line of Defense), in collaboration with the process owners (First Line of Defense), through an understanding of the activities, context, and objectives of each process.

Each identified risk must be classified and recorded under one of the following categories:

- a) **Strategic:** risks related to the Company's strategic decisions aimed at achieving long-term business goals such as expansion, market growth, and innovation. These may stem from internal factors (e.g., lack of capacity or management decisions) or external factors

(e.g., market, political or economic changes) that may compromise the Company's success and sustainability;

- b) Operational:** risks associated with the Company's operations (people, processes, and technology), affecting operational efficiency and the effective and efficient use of resources. They may arise from internal sources (e.g., fraud, human error, system failures, process inadequacies, business interruptions, misconduct, production or distribution incapacity) or external sources (e.g., natural disasters, cyberattacks, supplier failures), potentially resulting in financial loss, regulatory fines, legal and reputational impacts;
- c) Financial:** risks associated with financial/accounting operations and the reliability of the balance sheet. They may result from ineffective cash flow management, suboptimal financial returns, poor investment/funding decisions, or the issuance of inaccurate, incomplete, or untimely financial, managerial, or tax reports, exposing the Company to penalties. Key financial risks include credit, liquidity, market, and foreign exchange risk.
- d) Regulatory or Compliance:** risks related to non-compliance with applicable laws and regulations, including sector-specific rules, general domestic and international legislation (e.g., environmental, labor, civil, and tax laws), agreements, codes of conduct, and internal policies;
- e) Social and Environmental:** risk of losses resulting from adverse impacts on the environment or society, including harm to native populations, biodiversity, public health, and cultural property;
- f) Reputational:** risks that may damage the Company's brand, credibility, or public image due to actual or perceived negative events, including unfavorable media coverage, regardless of its accuracy;
- g) Information Risk:** risk related to loss or misuse of confidential or personal data, compromising the security and integrity of information, affecting its confidentiality, availability, and authenticity. These may stem from cyberattacks, human error, system failures, or natural disasters;
- h) Information Technology Risk:** risk of system or hardware failures that may impact the Company's operations and activities.

4.3 Evaluating and Prioritizing Risks

Once risks have been identified and classified, they must be assessed based on two dimensions:

- a) **Probability:** the likelihood of the risk materializing within a given time horizon;
- b) **Impact:** the severity of the consequences should the risk materialize.

Each risk is then rated on a scale of five levels for both dimensions and categorized into one of three risk levels, as illustrated in Figure 2:

- a) **High Risk:** requires immediate or short-term mitigation measures and/or implementation of internal controls;
- b) **Medium Risk:** requires short- to medium-term mitigation measures and/or implementation of internal controls;
- c) **Low Risk:** Prioritized after addressing high and medium risks through the implementation of respective actions and controls.

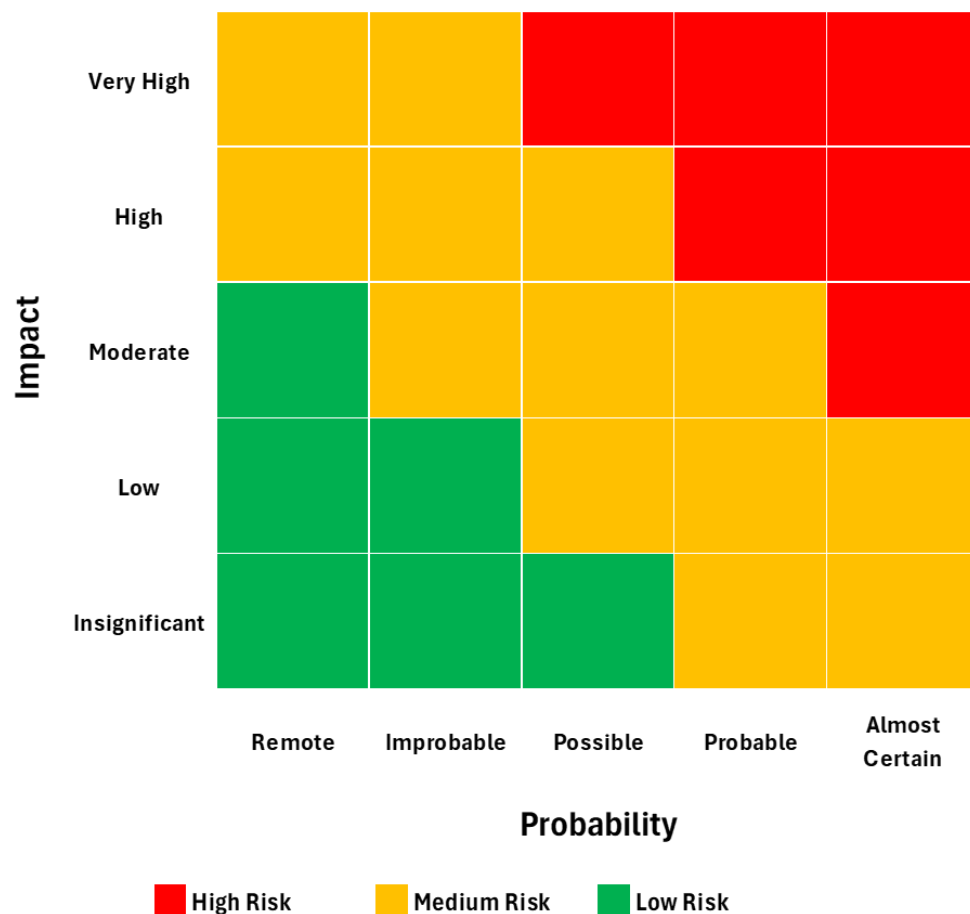


Figure 2: The Risk Assessment Matrix

To carry out this stage of risk assessment and prioritization, the following aspects should be taken into account:

- a) Regardless of the risk classification, consider the potential socio-environmental impacts if the risk materializes;
- b) Efficiency of existing internal controls, which requires an evaluation of their effectiveness. This includes aspects such as: risk mitigation, timeliness, segregation of duties, error detection and treatment procedures, automation, among others;
- c) Frequency with which the process is exposed to the risk;
- d) Possible disruptions to the Company's operations if the risk materializes;
- e) Potential financial losses if the risk materializes;
- f) Potential reputational damage if the risk materializes;
- g) Potential fines, legal actions, loss of benefits, or embargoes if the risk materializes.

4.4 Responding to Riskst

Based on the assessment performed in the previous stage, the response to each risk should fall into one of the four treatment categories listed below:

Avoid: discontinue the activities that generate the risk. This approach is used when there are no acceptable or viable alternatives to reduce the impact or probability of the risk, justifying the termination of the risk-generating process.

Mitigate: implement measures to reduce the probability of occurrence and/or the impact of the risk.

Transfer: reduce the probability of occurrence or the impact of the risk by transferring or sharing a portion of it—through insurance, hedging, partnerships, outsourcing activities, among others.

Accept: no measures are taken to affect the probability or impact of the risk; however, the event must be monitored through internal controls and periodically reassessed.

Internal controls are essential elements in the “mitigate” and “transfer” strategies and must therefore be evaluated, enhanced, or implemented (if not already in place). In other words, internal controls play a fundamental role in corporate risk management and must be mapped and managed by the Company, just like the risks they aim to mitigate.

4.5 Monitoring Risks and Internal Controls

Once risks have been assessed and internal controls reviewed or implemented, the process moves into cyclical monitoring to verify the effectiveness of the controls and, consequently, the accuracy of the risk assessments.

The identified risks and corresponding internal controls will be consolidated into Unicasa's risk matrix and internal control matrix to facilitate monitoring and management.

Regarding risks, the Company—through its Internal Controls, Risk and Compliance area (Second Line of Defense)—will periodically conduct reviews, which may include reclassifying risk levels and identifying emerging risks. This step involves monitoring changes in both external and internal environments and continuously improving event analysis and risk assessment processes.

As for internal controls, monitoring will be conducted through testing performed by the Internal Audit function, based on the Company's internal control matrix. This includes defining samples and collecting evidence of control effectiveness, in accordance with a pre-established calendar.

4.6 Communicate

The purpose of this final stage is to foster a culture of transparency, accountability, and risk awareness, while ensuring clear, objective, and timely communication to all relevant stakeholders. This may include issuing reports, disclosures, and other forms of communication.

5. RESPONSIBILITIES

As the process of corporate risk management permeates all business processes, all Unicasa employees are responsible for managing the Company's risks—both in defining strategies and projects, and in performing their daily activities.

The organizational structure for risk and controls management is shown below, based on the Three Lines Model developed by The IIA.

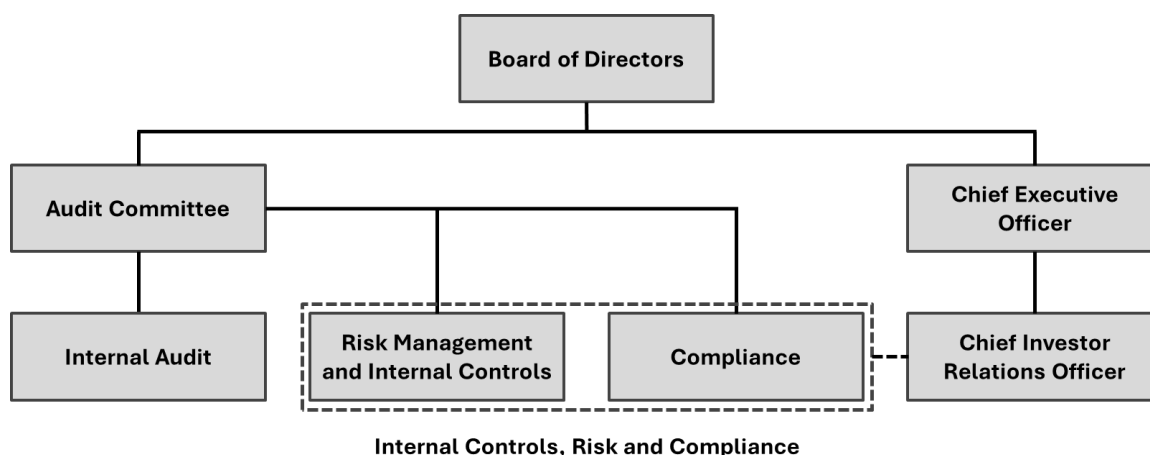


Figure 3: Organizational Chart – Internal Controls, Risk and Compliance

5.1 Board of Directors

The Board of Directors has the following responsibilities in relation to risk management:

1. To direct and instruct the activities related to the Company's risk management policies, through the Audit Committee;
2. To supervise the Company's Corporate Risk Management processes, including risk exposure, effectiveness of internal controls, and Compliance;
3. To define the Company's risk appetite, based on strategic guidelines, objectives, and projects;
4. To monitor the Company's principal risks as reported by the Audit Committee;
5. To ensure that the Company has an adequate Auditing (Internal and External), Governance, Risk and Compliance structure compatible with its size and complexity;
6. To approve the risk management policy, including any revisions or amendments;
7. To define and approve the responsibilities of the internal audit function.

5.2 Audit Committee

The Audit Committee has the following responsibilities in relation to risk management:

1. To supervise the activities, effectiveness, progress, and structure of the Company's corporate risk management, and suggest improvements to the Board of Directors;
2. To monitor and assess the Company's risk exposure, and, when necessary, recommend changes to the risk matrix and/or the Company's risk appetite levels, as well as to the internal controls structure designed to mitigate risks;
3. To define and manage the risk management communication and reporting process;

4. To define and approve the internal audit work plan;
5. To ensure and supervise the independence and absence of conflicts of interest between the Company's three lines of defense (especially between risk management and internal audit);
6. To periodically review this risk management policy and, if necessary, submit suggestions for changes to the Board of Directors;
7. To act in accordance with the responsibilities and provisions of the Internal Regulations of the Audit Committee.

5.3 Executive Board

The Executive Board has the following responsibilities in relation to risk management:

1. To accompany and sponsor the corporate risk management process, supporting awareness and engagement initiatives among the Company's leadership, based on the IIA's Three Lines Model;
2. To ensure the integration of corporate risk management into the Company's strategy design, monitoring, and review processes.

5.4 Employees (First Line of Defense)

The responsibilities of Unicasa employees regarding risk management are:

1. To manage risks in their day-to-day activities by identifying, assessing, and implementing mitigation actions (internal controls), as well as supporting the initiatives conducted by the Company's risk management experts;
2. To report events or situations that represent risks to the Company's risk management area and/or their immediate manager;
3. To actively participate in all risk management culture dissemination initiatives, including communications and training sessions.

5.5 Internal Controls, Risk and Compliance (Second Line of Defense)

The Internal Controls, Risk and Compliance area has the following responsibilities:

1. To assess and review risks identified by the business areas responsible for the processes, as well as the internal controls designed to mitigate those risks;

2. To coordinate the Company's Corporate Risk Management process, identifying, classifying, evaluating, and responding to risks jointly with the business areas responsible for the processes, taking into consideration the risk appetite defined by the Board of Directors;
3. To consolidate and keep the Company's risk matrix up to date, constantly monitoring the risk environment and reporting newly identified risks to the Audit Committee;
4. To prepare and maintain the internal controls matrix, evaluate the controls, and advise business areas on strengthening the Company's internal control environment;
5. To develop and apply the corporate risk management methodology, based on best market practices and in compliance with external laws and regulations, and internal policies and procedures;
6. To promote a culture of transparency, accountability, and risk awareness within the Company;
7. To periodically report on corporate risk management activities to the Company's Audit Committee.

The Compliance function also supports risk management through the implementation of tools such as the Code of Conduct, Ethics Committee, Whistleblower Channel, among others.

5.6 Internal Audit (Third Line of Defense)

The Internal Audit area has the following responsibilities:

1. To develop the annual internal audit plan for presentation to and approval by the Audit Committee;
2. To independently, impartially, and timely examine and test the effectiveness and quality of the Company's corporate risk management process, recording weaknesses and making recommendations for improvement;
3. To assess and test the design of existing internal controls, evaluating their effectiveness in mitigating associated risks;
4. To assess the internal controls environment and matrix, testing the effectiveness of the controls and recommending improvements, when necessary;
5. To identify and highlight any potential risks not yet mapped by the Company through monitoring and evaluation of the risk management and internal control processes;
6. To follow up on the implementation of recommendations made during the audit/evaluation of the risk management process and internal controls environment;

7. To provide information and reports to the Audit Committee on the effectiveness of the Company's risk and internal control management, as well as compliance with laws and regulations, classifying any identified deficiencies by severity.

6. GENERAL PROVISIONS

This Policy was implemented on April 28, 2022, and revised on May 30, 2025, by the Company's Board of Directors. It is effective for an indefinite term and shall remain in force until otherwise decided by the Board of Directors.