ORGANIZATIONAL POLICY

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 01
Responsible Management: Internal Controls, Risks and Compliance Management	**Published on:** 19/06/2019
Related rules:	**Review by:** 19/06/2021

1. Purpose

This policy aims to establish the principles, guidelines and responsibilities to be observed in the corporate risk management and internal control process, in order to ensure the proper identification, analysis, evaluation, treatment, monitoring and communication of corporate risks.

This document does not establish the risk appetite framework and acceptable limits of the Company for each type of identified risk, nor present a definition of risks and procedures for management and reporting, since confidential and operational management aspects are considered, whose definitions are described in the internal risk management standard.

2. Scope

This Policy applies to the TOTVS Group (TOTVS S.A and its controlled companies in Brazil and abroad, including affiliates and subsidiaries).

3. References

CODEC: TOTVS' Code of Ethics and Conduct, which aims to establish the conduct and ethical principles that guide TOTVS' commitment to business integrity and internal and external relationships.

COSO Internal Controls - Committee of Sponsoring Organizations of the Treadway Commission: a non-profit organization dedicated to improving financial reporting through ethics, effective internal controls and corporate governance, to prevent and avoid fraud in the company's financial statements.

COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management Framework — Methodology developed by COSO for the mapping and management of corporate risks.

ABNT (Brazilian National Standards Organization) NBR ISO 31000:2018: Risk Management — Principles and Guidelines.

IBGC (Brazilian Corporate Governance Institute): Corporate governance booklets, corporate risk management: Evolution in Governance and Strategy.

4. Concepts

Risk: An event that may adversely affect the Company's results and its ability to achieve its strategic and business objectives.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Inherent risk: level of risk intrinsic to the business or activity, without considering the implementation of mitigating controls.
Residual risk: level of risk calculated considering the implementation of mitigating controls.
Risk Sheet: document that formalizes the risks identified to Management, with a detailed description of the risk, its impact, probability and final classification.
Opportunity: an event that can positively impact the undertaking of Company objectives, contributing to the generation and conservation of value.
Risk factor: internal or external factors that may give rise to risks.
Risk tolerance: maximum level of exposure to risks that the Company is able to incur in taking advantage of opportunities and pursuing and carrying out its strategy.
Control activities: periodic or continuous activities performed to mitigate a risk. They comprise policies, standards and procedures to ensure that the guidelines and objectives, defined by the Company to minimize its risks, are being observed in the activities performed. Control activities occur at all levels of the Company.
Culture of risk Management: a set of accepted ethical standards, values, attitudes and behaviors, and the propagation of risk management as part of the decision-making process at all levels.
***Control Self Assessment*:** questionnaire answered by the managers of the departments responsible for internal processes and controls, in order to attest to the reliability of the information provided in the mapping of internal processes and controls and the documentation provided for design effectiveness tests (*Walkthroughs*).
Lines of Defense: a concept that defines roles and responsibilities in risk management and governance strengthening, as well as the interaction of these roles with all levels of the Organization.
Risk owner: responsible for the execution of internal controls to ensure that the risk is properly managed and for the definition and implementation of the necessary action plans for remediation and/or minimization of risks, as well as for the continuous monitoring and identification of new risks.
Risk exposure: quantification of the possibility of the Company being affected by a certain risk.
Risk management governance: refers to the Company's risk management roles and responsibilities, from the employees involved in the execution, who must be responsible for controlling direct risks in their activities, to the members of the Administration, Audit Committee and Board of Directors. The flow of information related to risk control and the transparency of such data, from identification to reporting to competent authorities.
Internal controls: the set of manual and systemic activities and controls that make up a protective barrier so that operational and decision-making activities are carried out in a safe environment and for risks to be quickly identified and addressed.
Probability: qualitative or quantitative level that defines the likelihood of a risk event occurring.
Impact: refers to the result or consequence of a risk event occurring. The impact of the risk is analyzed in different areas, according to the defined rule.
Action plans: actions or set of actions aimed at mitigating or reducing the level of exposure of an identified risk.
Risk matrix: consists of an inventory of the risks mapped by the company, classified according to their probability and impact.
Evaluation Cycle: refers to the annual cycle of identification, evaluation, analysis, treatment, monitoring and reporting of risks.

5. Guidelines

- The risk management process follows the Company's ethical principles, values and culture, and the information generated by the risk management system must be reliable, follow the legal guidelines, and

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

provide aid for decision making aimed at the mitigation or reduction of risk exposure level and proper prioritization of actions.

- The information used to manage risks and internal controls should be whole and correct, representing the current state of Company operations, so that all employees understand their role within the control structure and have available the necessary and authoritative information for the execution of their activities and management of risks.

- The risks of the Company must be communicated and known to all those involved in its management and monitoring, as well as be reported in a timely manner. The risk communication process should be clear and efficient, and comprise sufficient information for appropriate decision making.

- It is up to the management bodies to provide the means of implementing the processes of identification, evaluation, analysis, treatment, monitoring and control of risks.

- Risk mitigation depends on the implementation of controls, systems and protection mechanisms that do not have a single form or framework, and those that best adapt to the respective processes, as well as the structure and available resources, should always be prioritized.

All information and reports resulting from the risk management process are classified as restricted to internal use and must be adequately stored and safeguarded. The information to be reported externally, such as the Reference Form and Integrated Report, should reflect the methodology and results of the exposure identified in the risk management process.

5.1 Risk Category

The Company categorizes its risks according to the guidelines below, and considers external and internal factors in each category:

Strategic Risk: risk events associated with strategic decisions that affect the Company's business strategy or strategic objectives, considering the internal and external environment.

Operational Risk: Operational risks refer to possible losses resulting from failures, deficiencies or inadequacy of internal processes, people, or the technological environment, or losses caused by external events.

Financial Risk: connected to the Company's potential financial loss exposure, as well as to the reliability of accounting entries and financial statements. Such risk may arise, for example, as a result of the non-effectiveness in cash flow management aimed at maximizing and generating operating cash, business losses, customers' defaults, financial transaction returns, fluctuations in market indices applied to its contracts, gathering/application of financial resources, and the possibility of issuing incomplete, inaccurate or late financial, management or tax reports, exposing the Company to fines and penalties.

Regulatory/Compliance Risk: risks arising from legal or regulatory sanctions and financial or reputational loss that the Company may suffer as a result of failure to comply with laws, agreements, regulations and the Code of Ethics and Conduct, among others.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Information Technology Risks: risks related to the information technology environment (infrastructure, access management, data security) that may impact the Company's business, such as the occurrence of cyber attacks, leakage and/or loss of data integrity, IT environment downtime, and technological obsolescence.

5.2 Risk Management Process and Methodology

The methodology applied in the Company is supported by the components described in COSO ERM (Enterprise Risk Management) and ISO 31000 and comprises six essential steps, as well as risk management culture and governance aspects, as detailed in the following items:

5.2.1 Establishment of the Context

The initial stage of the risk management process, which comprises the capture and understanding of the Company's short-, medium- and long-term strategic objectives, considering the internal and external environment.

5.2.2 Risk Identification

The process of capture and identification of risks consists of the use of specific methods, such as process mapping, interviews with the responsible managers of each area/business segment and the collection of losses occurred in the past, in order to establish risk matrices and controls and keep them regularly updated, based on the events that may impact the Company's strategic and business objectives.

5.2.3 Risk Analysis and Assessment

The risks should be assessed according to their impact and probability, as well as the associated risk factors, considering the following assumptions:

- Impact: The impact assessment should consider the analysis of each identified risk factor, forecasting the consequences of a given risk's manifestation in each of the following areas: (i) Finance; (ii) Reputation; (iii) Legal/Compliance; and (iv) Interruption of Operations. The areas are classified independently, and among the four areas, the greatest impact must be considered for determining the final classification of the risk in the matrix. Classification of the possible impact is determined by the application of a severity scale, in four levels: Low; Medium; High; and Very High.

- Probability: level of exposure that considers the qualitative analysis of the professional responsible for risk assessment, as well as the history of occurrence frequency, if any, and the current status of the risk factors identified. The probability classification is determined by the application of an occurrence expectation scale, in four levels: Low; Medium; High; and Very High.

The risk's final classification is determined by intersecting the probability and impact axes, resulting in five levels: (i) Very Low; (ii) Low; (iii) Medium; (iv) High; and (v) Critical, as shown below:

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 01

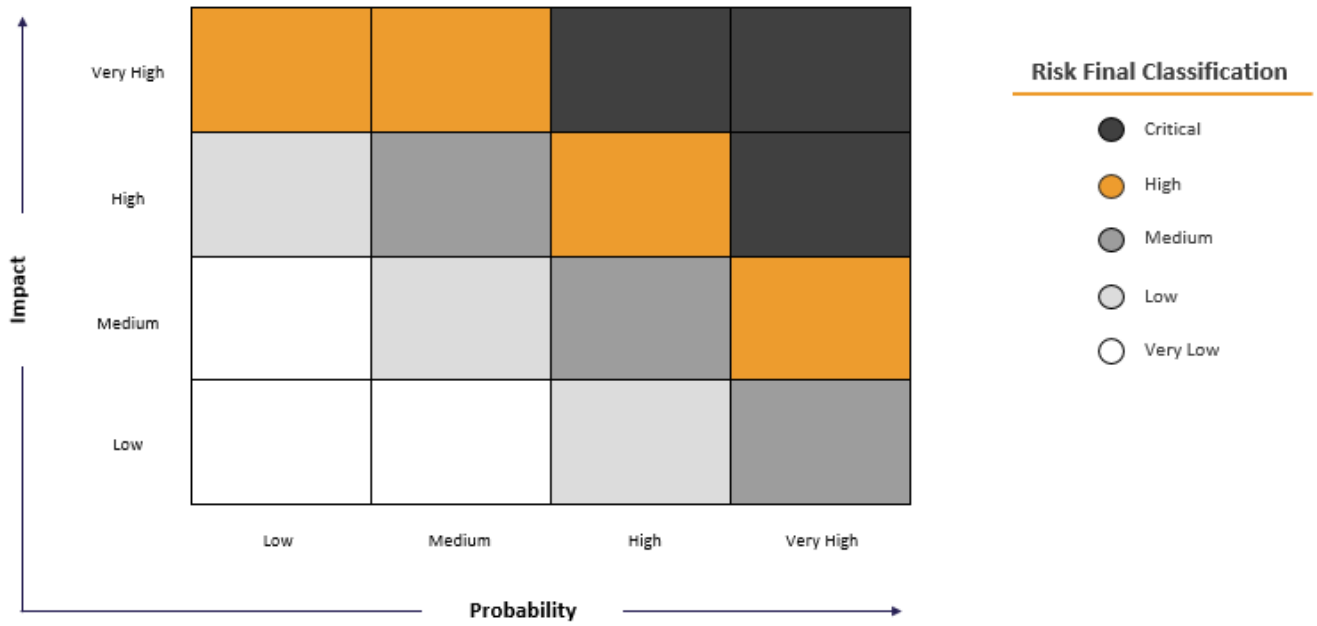

Figure 1: Probability and impact classification matrix.

5.2.4 Risk Treatment

Identified risks must be adequately managed and the formulation of the response should be carried out according to the severity. This phase involves the selection, formalization and implementation of one or more action plans to reduce or mitigate risk events by the respective responsible areas.

High and Critical risks should be subject to reduction or risk mitigation action plans, with a maximum term of 60 days from their identification for the initial actions that reduce the risk classification, except for plans that depend on unavailable resources, highly complex IT projects or organizational change, in which case the deadlines may be extended, with the approval of the Audit Committee, and acceptance of the residual risk as high or critical should be submitted, on the recommendation of the responsible area's Vice-President and the Chief Executive Officer, for the knowledge and approval of the Board of Directors.

5.2.5 Monitoring and Reporting

Adequate risk monitoring involves the constant monitoring of the Company's control environment and risk response actions (action plans).

The internal control structure should be evaluated periodically, verifying the efficiency of existing internal controls and the effect of potential changes in the Company's internal environment and/or external environment.

The improvement actions (action plans) and their effectiveness must be backed by the responsible areas with the support of the Internal Controls, Risks and Compliance Management, through quarterly follow-ups presented to the Audit Committee. Deadline extension for the completion of action plans must be preceded

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

by formal justification by the responsible area and duly reported to the Audit Committee. For High and Critical risks, the Audit Committee must be informed of the requested extension and inform the Board of the reasons and the new forecast for completion of said plans.

5.3 Internal Controls

Internal controls contribute to the mitigation of risks, providing a safer and more efficient environment, in terms of operational efficiency and integrity of records and information, mainly considering the following aspects: (i) the Company's strategic objectives; (ii) composition and nature of the accounts; (iii) possibility of losses due to errors and fraud; and (iv) complexity in the transactions of the accounts.

In order to achieve its objectives, the Company's internal control management is structured in an integrated model of Three Lines of Defense:

- 1st Line of Defense: The Business Areas, responsible for identifying and reporting the risks of their operations and ensuring that they meet their business objectives, as well as the proper functioning of their internal control structure;

- 2nd Line of Defense: Internal Controls, Risks and Compliance Management, using the supporting documentation produced by the 1st Line of Defense as an aid in reviewing the control environment. It acts in an advisory way, supporting the business areas in the development and implementation of processes and controls;

- 3rd Line of Defense: The Internal Audit, responsible for independently analyzing and evaluating the internal control environment based on the work performed by the 1st and 2nd lines of defense. It may perform additional tasks as needed.

5.3.1 Stages of Internal Control Management

The Internal Controls, Risks and Compliance Management is responsible for process mapping, controls and walkthrough tests, in order to check the understanding of the mapped processes, and if the controls are implemented and functioning properly.

Controls that are absent or considered unsatisfactory in mitigating the risks identified in the business processes are reported to the responsible areas for the preparation of action plans (be it the creation of the new control or the improvement of the existing controls).

Once these steps are completed, those responsible for the processes must annually carry out the Control Self Assessment, as well as provide proof of the implementation of controls in the system used by TOTVS and, where appropriate, point out new risks identified by the controls' processes or activities.

The processes and controls mapped out by the Internal Controls, Risks and Compliance Management are a fundamental tool for Internal Audit planning. Based on the mapping, Internal Audit defines the strategy and the effectiveness tests that will be carried out (called "Control Tests"), with the objective of evaluating the controls' correct application and operational efficiency in the prevention or detection of relevant distortions.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

All mapping processes and control reviewing, and their respective results, are reported to the Company's Audit Committee.

6. Responsibilities

Board of Directors

- Define the strategic objectives of the company that will guide the organization's risk identification work;
- Approve the Risk Management and Internal Control Policy;
- Approve the company's risk management and internal control methodology;
- Monitor the actions of risk management according to the Company's business direction;
- Determine and validate the review cycles of the risk control system and their effectiveness;
- Determine risk tolerance;
- Approve the risk map (strategic and operational) and the main risk factors to which the Company is exposed;
- Validate public information documentation on the risk management model and transparency of information provided to the internal and external public.

Audit Committee

- Propose changes to the Risk Management and Internal Control Policy and submit them to the Board of Directors;
- Assist Management in defining guidelines and methodology for risk management and internal controls, in addition to metrics for measuring tolerance and risk appetite, presenting to the Board of Directors its recommendation for approval;
- Evaluate prepared action plans for risks classified as "high" and "critical".
- Monitor and recommend to the Board of Directors the acceptance of responses to high and critical risks;
- Evaluate the risk map (strategic and operational) and the main risk factors to which the Company is exposed, presenting its recommendations to the Board of Directors;
- Supervise and periodically monitor the results of control tests and mitigation action plans, reporting to the Board of Directors any deviations or occurrences deemed relevant;
- Monitor the actions of risk management according to the Company's business direction.

Internal Controls, Risks and Compliance Management

- Propose and apply the Risk Management methodology, creating an effective monitoring system;
- Conduct the identification, evaluation, treatment, monitoring and communication of strategic and operational risks with the relevant areas;
- Report Strategic and Operational risks to the Executive Board, Audit Committee and Board of Directors;
- Propose changes and submit the Risk Management and Internal Control Policy to approvals;
- Deliberate on recommendations proposed by the Risk Owners to minimize the risks of the Company in line with the strategy and defined objectives;
- Monitor the implementation actions of internal controls for risk management;
- Carry out the monitoring and quarterly reporting of all actions developed for risks classified as "Medium", "High" and "Critical";
- Monitor and periodically report the progress of the action plans developed;

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

- Map processes and assist in the identification of risks (e.g., operational and financial), and the respective controls that mitigate these risks;
- Monitor and suggest improvements to internal controls by the operating areas;
- Report any discrepancies or outdated process flow designs, standards and procedures whose changes may negatively effect the control environment;
- Educate managers on the importance of risk management and internal controls and the responsibility inherent to administrators, employees, interns and other TOTVERS.

Internal Audit

- Use the Risk Map to aid the annual audit plan of the processes of the Company and its subsidiaries and controlled companies;
- Audit the Company's Risk Management process with impartial, independent and timely opinions;
- Monitor the internal control environment and the effectiveness of risk management based on the work performed by the Business Areas and Internal Control, Risk and Compliance Management;
- Run the control tests according to audit planning and report the results to the Audit Committee;
- Check the implementation of action plans and their effectiveness;
- Identify the need to prioritize actions based on the results of ongoing risk processes, as well as broaden the scope of substantive testing or continuous monitoring in light of new risks or worsening of previously mapped risks;
- Identify and point out opportunities for improvement in internal control and risk management processes;
- Issue a formal opinion on the internal controls tested in the annual audit cycle.

Owners of Risks/Business and Operational Areas

- Continually identify and document the risks under their management;
- Carry out the Control Self Assessment and provide the necessary proofs;
- Annually evaluate the performance and results of the risks and controls under its management;
- Communicate any newly identified risks and any changes in its business process to Internal Controls, Risks and Compliance Management;
- Establish appropriate controls for risk management;
- Execute action plans under its responsibility;
- Ensure that the implemented actions are effective and result in reducing the degree of risk exposure at acceptable levels.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 01

7. Approvals (Document)

Name/Position	Description
Marcos Corradi Manager of Internal Controls, Risks and Compliance	Development
Ricardo Guerino Director of Planning, Controllership, Internal Controls, Risks and Compliance	Review
Claudia Karpat Legal Officer	Review
Gilsomar Maia Sebastião Executive Financial Vice President	Review/Recommendation
Audit Committee	Recommendation
Board of Directors	Approval

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©