Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00
Department: Internal Controls, Risks and Compliance Department	**Published on:** 06/07/2017
Related standards:	**Review:** 06/07/2019

1. Purpose

This policy establishes the guidelines and responsibilities to be complied with in the risk management activities of TOTVS in order to ensure that the risks inherent to the Company's activities are identified, assessed, addressed, monitored and reported to Management in a timely manner for decision-making, thereby minimizing the impact of the risk or better exploring opportunities through internal controls and adequate risk governance.
This document does not establish the Company's risk appetite model and acceptable limits for each type of risk identified, nor does it provide a dictionary of risks and procedures for management and reporting, since confidential and operating management aspects are considered, the definitions of which are described in a risk management standard for internal use.

2. Scope

This Policy applies to all areas of the TOTVS Group (Head Office, Subsidiaries, Own Units, Branches and Franchises). Compliance with these guidelines is mandatory.

3. References

COSO – Committee of Sponsoring Organizations of the Treadway Commission: a non-profit entity dedicated to improving financial reports through ethics, effectiveness of internal controls and corporate governance in order to prevent and avoid fraud in the financial statements of companies.
COSO ERM – Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management Framework – A methodology developed by COSO to map and manage corporate risks.
Corporate Risk Management – IBGC: Evolution in governance and strategy

4. Concepts

Risk: Possibility of occurrence of an event that affects the company's ability to achieve its objectives;
Opportunity: An event that could positively impact the achievement of the Company's objectives, contributing to value creation and preservation;
Risk factor: Internal or external factors that could originate risk events;
Risk appetite: The level of risks the Organization is willing to accept to achieve its goals and objectives and create value for the Company;
Risk tolerance: Deviations from the level of risks established as acceptable;
Control Activities: Policies, procedures, activities and mechanisms developed to ensure that the business objectives are achieved and to prevent, detect and correct undesirable events;

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

Risk culture: Set of ethical standards, values, attitudes and behaviors accepted and practiced, and the dissemination of risk management as part of the decision-making process across all levels;
Lines of defense: Concept that defines roles and responsibilities in risk management, and the strengthening of governance, as well as interaction of these roles across all levels of the Organization. The first line is represented by area and/or business managers, directly responsible for the execution of their processes and the respective risks. The second line is the Internal Controls and Compliance area, which identifies performance failures in controls and deviations from policies and internal procedures, and the third is the Internal Audit area, which runs substantial internal controls tests and identifies operating and financial deviations resulting from flaws and/or fraud;
Risk owner: Is responsible for identifying and effectively managing risks in their process or area of operation. The risk owner should have established roles and responsibilities to choose and implement responses to these risks, as well as sufficient authority to prioritize risk management actions in their area and be integrated to the company's overall risk governance process;
Risk exposure: possibility of the Company being affected by a certain risk;
Risk management governance: Relates to the roles and responsibilities of each of the Company's corporate governance agents, from employees involved in the execution, who must be responsible for controlling the direct risks of their activities, to members of the Board of Directors, Audit Committee and Board of Executive Officers. The flow of information related to risk control and transparency of this data is also part of the company's Risk Management governance, which determines the decision forums, the powers of these forums, their roles and responsibilities and their composition;
Internal controls: The set of activities and manual and systemic controls that provide a protective barrier so that operations and decision-making processes are made in a secure environment, where interference and risks are swiftly identified and addressed.

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, comply with legal provisions and support decision-making processes to reduce the level of exposure to risks and prioritize actions;
- Management bodies are responsible for ensuring sufficient resources to execute the processes of identifying, assessing, addressing and monitoring risks;
- Mitigation of risks depends on the implementation of controls, systems and protection mechanisms that have no unique format or model, always prioritizing the one that best adapts to the process, structure and resources available at the time of activation;
- Major risk events or risks that are unacceptable for the Company that could compromise its perpetuity, reputation and values, must include in their management, business continuity management, crisis management, as well as risk sharing initiatives, such as the contracting of insurance coverage;
- All information and reports resulting from the risk management process must be adequately filed and safekept. Such information must be classified as information restricted to internal use, and externally reported information, such as the Reference Form and Integrated Report, must reflect the methodology and results of exposure identified in the risk management process.

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

Risk Category

TOTVS classifies its risks based on the following guidelines and considers both external and internal factors in each category:
Strategic Risk: risks that affect the strategic objectives, considering the internal and external environment;
Operating Risk: risks related to the Company's operations (processes, people and technology) that affect the operating efficiency and effective and efficient use of resources. These can take several forms, such as fraudulent actions, interruption of business, employee misconduct and deficiency in contracts, resulting in financial and business losses, fines and/or legal and reputational impacts;
Financial Risk: related to the exposure of the Company's financial/accounting operations and the reliability of its balance sheet. It can result from ineffective management of cash flows in order to maximize and generate operating cash, returns on financial transactions, funding/investment of financial resources, and possibility of issuing incomplete, inaccurate or untimely financial, management and fiscal reports, exposing the Company to fines and penalties;
Regulatory/Compliance Risk: risks related to compliance with rules and laws, considering the laws that apply to the industry of operation and legislation as a whole, both domestic and international (environmental, labor, civil and tax/fiscal).

Risk Management Methodology

The methodology used at TOTVS is supported by the components described in the COSO ERM (Enterprise Risk Management), namely: Risk governance and culture, Risk, strategy and definition of objectives, Identification, assessment and treatment, Information, communication and reporting, and lastly, Monitoring.
Risk Governance and Culture: The risk culture must be disseminated across all levels of the Company, and risk management and monitoring must not be an action exclusively taken by one executive or department. Managers are primarily responsible for the day-to-day management of risks related to their department or business process and the dissemination of risk management culture among their team members, managing exposure to risks through established action plans;
Risk, strategy and definition of objectives: the risk management strategy must include internal and external factors, as well as the impact of risks that may be in disagreement with the guidelines established by the Company and may affect the achievement of business objectives and strategy;
Identification, assessment and treatment: risks must be periodically identified, assessed, prioritized and documented in a structured manner so as to be adequately treated.;
Risks are categorized based on their nature and origin, in accordance with the risk categories. For this, the processes of identification, assessment and treatment of risks must be described.

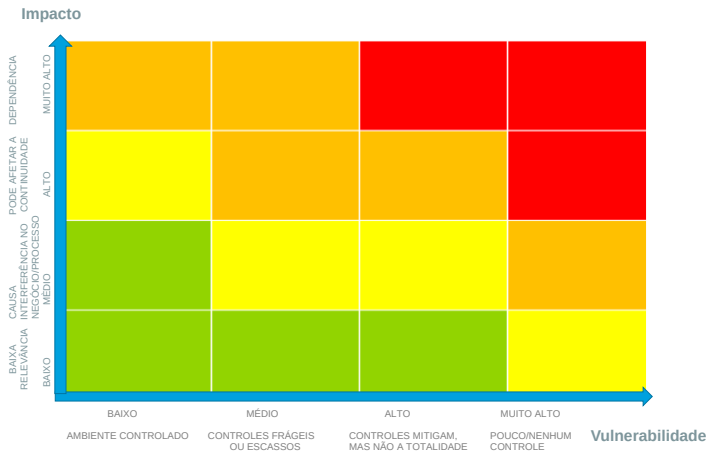
Identification: The process of capturing and identifying risks consists of using the COSO ERM (Enterprise Risk Management) tools and methodology to establish the risk and control matrices and keep them constantly updated. The Company must pay attention to the emergence of new risks and/or emerging risks which, after being identified, must be assessed, incorporated in the risk management process and, depending on their criticality, immediately reported and treated;
Assessment: Risks must be assessed according to their impact and vulnerability, considering the following assumptions, and the final risk classification will be defined after combining the result of vulnerability and impact.

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

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

Impact considers the analysis of risk in relation to the possible impact on the Company's operations. The criterion for determining the impact will be applied in accordance with qualitative assumptions that could affect, for instance, the value created for stakeholders (impact on clients, suppliers and investors); the Company's reputation and Image; non-compliance with the law and resulting fines and other penalties.
Vulnerability, on the other hand, considers an analysis of the risks regarding the magnitude of the Company's exposure or lack of protection from risks, considering: (i) the effectiveness of internal controls; (ii) the level of management's influence regarding the risk factor and risk; (iii) speed at which the risk can materialize; (iv) history of materialization of risk, among others.

For the analysis phase, these aspects are scored according to the following classification criteria:



Treatment: The risks identified must be correctly managed and the response must be defined according to their criticality. The response must consider the impact/vulnerability and cost/benefit ratios to adequately mitigate the risk.
Reducing the risk: Risks that may significantly impact the Company's strategic objectives and/or its operation. These risks must be controlled and reduced to acceptable levels through process improvements and effective internal controls directly related to the risk factor.
Accepting the risk: Risks whose impact is lower than the cost/benefit of their management may be maintained, provided they are known and accepted by the Audit Committee and by Senior Management. However, monitoring must be continuous and, if the impact or vulnerability increases, new decisions regarding the treatment of these risks must be made.

Information and communication: Information used to manage risks must be complete and accurate, representing the current situation of the Company's operations, so that all employees understand their role within the control structure and have the necessary and correct information available to carry out their activities and manage their risks. The Company's risks must be communicated to and known by all those involved in their management and monitoring, and must be reported in a timely fashion. The risk communication process must be clear and efficient, and the content of information must be sufficient for the decision-making process.

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

Monitoring: Risks must be continuously monitored to prevent the Company's exposure to risks from increasing and hindering business continuity. Adequate risk monitoring consists of constantly overseeing the Company's control environment and risk response actions.
The internal control structure must be periodically assessed to check the efficiency of existing internal controls and influences resulting from potential changes in the Company's internal and/or external environment.
Improvement actions (action plans), as well as their effectiveness, must be monitored to guarantee the achievement of the initial purpose, implementation deadline and efficient risk reduction. This assessment must be carried out once every six months for risks considered to very high and high, and annually for medium and low risks. With regard to TOTVS' strategic planning, a systemic review of the risk management process must be carried out by an external agent.

6. Responsibilities

Board of Directors

- Define the company's strategic objectives that will guide the task of identifying the organization's risks;
- Monitor risk management actions in accordance with the Company's business objectives;
- Determine and validate the revision cycles of the risk control system and their efficiency;
- Determine the risk appetite and tolerance;
- Validate documents containing public information about the risk management model and transparency of the information provided to internal and external stakeholders;
- Allocate the necessary resources for risk management.

Audit Committee – Technical advisory committee of the Board of Directors

- Monitor and recommend about acceptance of responses to risks;
- Help Management define the risk management guidelines and metrics for measuring risk tolerance and appetite;
- Approve the dictionary of risks, common language of risks and strengthen the risk management culture;
- Monitor risk management actions according to the Company's appetite;
- Monitor and encourage the development of risk protection structures and mechanisms;
- Propose changes to the Risk Management Policy and submit them to the Board of Directors;
- Ensure the functioning of mechanisms and controls related to risk management;
- Ensure the coherence of financial policies with strategic guidelines and risk profile of the business;
- Report its conclusions to the Board of Directors.

Board of Executive Officers

- Approve the risks assumed under its authority and, if necessary, submit them to the Audit Committee.
- Determine the Company's Risk Management Methodology;
- Monitor the actions to implement internal controls for risk management;
- Raise awareness among TOTVERS about the importance of risk management.

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

Risk Management Department

- Identify, assess, treat, monitor and communicate strategic risks to applicable departments;
- Monitor the status of Strategic, Operating, Financial and Regulatory Risks (Compliance);
- Propose changes to the Risk Management Policy and submit it for approvals, and also prepare and update the standards and procedures related to risk management;
- Propose and lead the implementation of operating procedures related to risk management, in line with the guidelines established by Management;
- Discuss the recommendations proposed by Risk Owners to mitigate the company's risks, in line with the strategy and objectives established;
- Monitor the actions to implement internal controls for risk management;
- Consolidate the assessment of the Company's risks by preparing periodical reports and submitting them to the Board of Executive Officers, Audit Committee, Strategy and Technology Committee and Board of Directors;
- Raise awareness about the importance of risk management and the inherent responsibility of managers, employees, interns and other TOTVERS.

Internal Audit

- Audit the Company's Risk Management process with impartial, independent and timely reports;
- After the implementation of action plans, audit the actions to check if they were all implemented as planned;
- Identify new opportunities and processes that can be prioritized based on the results of the risk process in progress, as well as expand the environment of substantial tests or continuous monitoring based on the identification of new risks or worsening of previously identified risks.

Internal Controls

- Map the processes and help identify risks (operating and financial, for instance), in addition to the respective controls that mitigate these risks;
- Monitor and suggest improvements to internal controls by operating departments;
- Report inconsistent or outdated process flows, standards and procedures whose changes could worsen the control environment.

Risk Owners/Business and operating areas

- Identify and document business risks;
- Annually assess the performance and results of risks under their management, especially with regard to the revision of risks incurred that significantly deviate from expected parameters;
- Communicate to the Risk Management department any new risks identified and any changes in business processes for analysis and identification of new risks and their respective controls;
- Establish adequate controls for risk management;
- Comply with the action plan;

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

Subject: Risk Management and Internal Controls	**Identification:** PO-GC-03 Version: 00

- Ensure that the actions implemented are effective and result in exposure to risks being reduced to acceptable levels.

7. Approvals (document)

Name / Position	Description
Manuela Loeser Manager - Internal Controls, Risks and Compliance	Preparation
Silvio Roberto Reis de Menezes Executive Officer - Ombudsman, RCC, Processes, Risks and Compliance	Preparation and Revision
Andre Rizk Chief Legal Officer	Revision
Gilsomar Maia Sebastião Chief Financial Officer	Revision / Recommendation
Audit Committee	Recommendation
Board of Directors	Approval