ORGANIZATIONAL POLICY

Subject: Risk Management, Internal Controls and Compliance	**Identification:** PO-GC-03 **Version:** 05
Board in Charge: Internal Controls, Risks and Compliance	**Published on:** 05/05/2026
Related Rules:	**Review by:** 05/05/2029

1. Objective

The purpose of this policy is to establish the principles, guidelines, and responsibilities to be observed in the management of Corporate **Risks**, **Internal** Controls, and **Compliance**, as well as to promote a **Culture of Risk Management** and the **Integrity program** throughout all levels of TOTVS.

2. Scope

This Policy applies to all divisions of TOTVS, their respective employees and officers, as well as their wholly-owned subsidiaries; the rules set forth herein must be incorporated into the policies of direct and indirect subsidiaries, both in Brazil and in other countries, while always complying with their articles of incorporation and applicable local laws.

It must also be ensured that **Third parties**, subcontractors, representatives, consultants, suppliers, and service providers of any kind, when interacting with or representing TOTVS, also base their actions on the provisions of this Policy.

3. References

- ABNT (Brazilian National Standards Organization) NBR ISO 31000:2018: Risk Management — Principles and Guidelines.
- CODEC – TOTVS Code of Ethics and Conduct.
- Brazilian Code of Corporate Governance of Publicly-held Companies – Brazilian Institute of Corporate Governance – "IBGC".
- COSO ERM – Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.
- Decree 11.129/22 – Decree regulating the Anti-Corruption Law.
- TOTVS Bylaws.
- IBGC: Corporate Governance, Corporate Risk Management and Compliance in the light of Corporate Governance booklets.
- Law 12.846/13 – Brazilian Anti-Corruption Law.
- CGU Ordinance 909 – Evaluation of integrity programs undertaken by legal entities.

4. Definitions

Action Plan: an action or set of actions aimed at mitigating or reducing the level of exposure to an identified risk; this may take the form of a project, a specific action, or a process control (ongoing action).
Annual Compliance Schedule: a plan designed to determine the prioritization of actions outlined in the Integrity Program.
Climate Change: refers to long-term changes in temperature and weather patterns, which may be caused by natural factors or result from human activities.

Compliance: derived from the English verb "to comply," which means conformity—that is, the duty to comply with and enforce laws, decrees, regulations, and instructions applicable to TOTVS's activities.
***Control Self-Assessment (CSA)*:** Control Self-Assessment is a methodology/technique used to evaluate the design and operational effectiveness of internal controls. It involves a questionnaire completed by business unit managers to self-assess both the internal controls and the risks associated with the processes under their responsibility.
Dictionary of Priority Risks: a standardized reference for identifying, categorizing, and organizing risk events that could affect the company's strategic objectives.
Employee or Employees: For the purposes of this Policy, this term refers to all employees who work at TOTVS.
Ethics and Conduct Hotline: a channel through which anyone who has a direct or indirect relationship with TOTVS (including employees, shareholders, customers, suppliers, franchisees, and partners, as well as their employees and any third parties) to confidentially report situations that may constitute a violation of the TOTVS Code of Ethics and Conduct or any other act that violates or may violate applicable laws and/or regulations.
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.
Integrity Program: a set of internal integrity mechanisms designed to prevent, detect, and combat fraud, corruption, and other illegal acts committed in the private or public sectors, in accordance with applicable regulations in Brazil and/or abroad, in the locations where TOTVS operates.
Internal Controls: a set of manual and systemic activities and controls that form a protective barrier to ensure that operational activities and decision-making take place in a secure environment and that risks are quickly identified and addressed.
Internal Regulatory Framework: consists of regulatory documents that establish policies, standards, guidelines, rules, procedures, templates, and methods designed to guide Employees' interactions in their daily activities, in line with TOTVS's values, culture, and strategy, and in accordance with applicable regulations.
Key Risk Indicators (KRIs): indicators used to measure and monitor data associated with risks, either of a predictive/preventive nature if there are metrics indicating that they are likely to materialize, or a detectable nature, in the case of indicators showing that the risks have already materialized.
Opportunity: an event that can positively impact the undertaking of Company objectives, contributing to the generation and conservation of value.
Probability: qualitative or quantitative level that defines the likelihood of a risk event occurring.
Public Entities: any agency or entity directly or indirectly linked to any branch of the national or foreign public administration, such as, but not limited to, the Federal Government, the Federal District, the states, the municipalities, and the diplomatic missions of foreign countries. This concept also includes legal entities controlled by these bodies or entities, even if they are organized under private law, such as local government agencies, state-owned enterprises, foundations, associations, and international organizations.
Risk Appetite: refers to the level of risk the Company is willing to take to achieve its strategic objectives. The Company's Risk Appetite is defined and measured on a qualitative basis.
Risk Exposure: quantification of the likelihood that TOTVS will be affected by a particular risk.
Risk Factor: internal or external factor that may give rise to Risks.
Risk Management Culture: a set of accepted and practiced ethical standards, values, attitudes, and behaviors, and the integration of risk management into the decision-making process at all levels.
Risk matrix: consists of a graphical representation of the inventory of mapped risks, classified in quadrants according to their materialization probabilities and their impacts.
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 tolerance: maximum level of exposure to risks that the entity is willing to incur in taking advantage of opportunities and pursuing and carrying out its strategy.
Risk: An event that could adversely affect TOTVS's results and its ability to achieve its strategic and business objectives.
Senior Management: members of the Board of Directors and the Executive Board.
Statutory Management: CEO and Vice Presidents of TOTVS.
Third Party(ies): any individual (other than an employee) or legal entity that has any relationship with TOTVS, including franchisees.
TOTVS or the Company: means TOTVS S.A., its subsidiaries and direct and indirect affiliates, individually or collectively, in Brazil or abroad, with the exception of TOTVS Techfin.

5. Guidelines

- TOTVS is committed to ethical conduct in its relationships with **Employees**, customers, partners, suppliers, investors, **Government Agencies**, and other stakeholders, and to compliance with applicable laws and regulations, including, but not limited to, anti-corruption laws and the Company's internal policies, standards, and procedures;
- The **Risk** management and Internal Controls process should provide input for decision-making aimed at mitigating or reducing the level of **Risk Exposure** and ensuring that actions are appropriately prioritized;
- The information used for **Risk** management and internal controls must be complete and accurate, reflecting the current status of TOTVS's operations;
- The Company's **Risks** must be communicated to all those involved in their management and monitoring, and reported in a timely manner.

The Internal Controls, Risk, and Compliance department reports directly to the CEO of TOTVS and enjoys the independence and autonomy necessary to carry out activities related to the **Integrity Program**, including unrestricted access to the information required to fulfill its responsibilities; these principles are reinforced by the support of TOTVS's senior management.

5.1. Risk Management

5.1.1. Risk Category

The Company classifies its **Risks** as described below, taking into account both external and internal factors.

Strategic Risk: Risk events associated with decisions that affect TOTVS Group's business strategy or strategic objectives, considering the internal and external environment.
Operational Risk: refers to potential losses resulting from disruptions, failures, deficiencies, or inadequacies in internal processes, personnel, the organizational environment, or technology, or caused by external events, including physical risks to facilities.
Financial Risk: This risk is associated with TOTVS's exposure to potential financial losses.
Regulatory/Compliance Risk: Risks of legal or regulatory sanctions, financial loss, or reputational damage that TOTVS may incur as a result of failure to comply with laws, agreements, regulations, the Code of Ethics and Conduct, and other requirements.
Information Technology Risks: Risks related to the information technology environment (including, but not limited to, infrastructure, access management, information security, and the use of artificial intelligence) that could impact TOTVS's business, such as cyberattacks, data breaches, IT system downtime, and technological obsolescence.

5.1.2. Risk Management Process and Methodology

The **Risk** management methodology applied at TOTVS is supported by a hybrid model that incorporates the components described in COSO ERM (*Enterprise Risk Management*) and ISO 31000. This approach establishes a framework for the integrated and continuous management of Corporate **Risks**, structured around six (6) essential stages, in addition to aspects of culture and governance, as detailed below:

5.1.2.1. Establishment of the Context

The initial stage of the process involves identifying and understanding strategic objectives, taking into account internal and external factors that may impact the achievement of these objectives over the short (1 year), medium (2 to 3 years), and long term (4 to 5 years), covering industry trends, technological changes, the macroeconomic landscape, the regulatory environment, sustainability issues, and climate change, as well as any other factors identified in the scenario analysis.

5.1.2.2. Risk Identification

The **Risk** identification process involves the use of specific tools, such as process mapping, interviews with managers responsible for each business area or segment and with senior management, as well as an analysis of past **Risk** events. This process should enable the identification of risks, with the aim of establishing risk matrices and keeping them constantly updated based on events that could impact TOTVS's strategic business objectives.

This step should also ensure a direct correlation between the identified **Risks** and TOTVS's material issues, taking into account financial and sustainability aspects, and using the **Dictionary of Priority Risks** as a standardized reference for categorization.

5.1.2.3. Risk Analysis and Assessment

Risks and their associated **Risk Factors** are assessed based on their **Probability** and **Impact**, taking into account the following areas:

- **Financial:** measures direct financial loss, taking into account the **Impact** on the company's operating results;
- **Reputational:** assesses the extent of negative exposure to TOTVS's image within its ecosystem (customers, partners, investors, and **Employees**) and the resulting impact on digital media or news outlets;
- **Legal/Compliance:** assesses the **Impact** of legal or regulatory sanctions, judicial or administrative proceedings, non-compliance with licenses or applicable laws, the Code of Ethics and Conduct, among other factors;
- **Operational:** measures the level of disruption to internal processes or the provision of services to customers, taking into account the time required to resume normal operations, including physical events that may impact operational continuity; and
- **Information Security:** assesses damage to the integrity, availability, and reliability of data belonging to TOTVS and its customers resulting from cyber incidents or data breaches.

For the consolidated classification of **Risk Probability** and **Impact**, the highest level of criticality identified for each of the analyzed **Risk Factors** shall prevail. The final risk rating is determined by plotting points on the **Probability** and **Impact** axes, resulting in four levels: (i) Low; (ii) Medium; (iii) High; and (iv) Critical. In addition, the analysis may consider the interconnectivity among the **Risks** in the matrix as a qualitative factor for understanding potential chain **Impacts**.

This document is the property of TOTVS. All rights reserved. ©
This document is the property of TOTVS. All rights reserved. ©

5.1.2.4. Risk Treatment

The definition of a risk response involves the development, formalization, and implementation of one or more **Action Plans** to mitigate **Risk** events by the respective responsible departments. The treatment should aim to reduce the **Probability** and/or **Impact** of the identified **Risks**, ensuring that the responses are effective and that resources are used optimally and in line with TOTVS's strategic objectives.

The treatment process is supported by potential enhancements to **Internal Controls** and the establishment of **Key Risk Indicators (KRIs)** linked to specific **Risks** or **Risk Factors**, with a single indicator capable of monitoring more than one event simultaneously. In cases where the indicator does not allow for the setting of quantitative targets, the assessment is based on a qualitative analysis of the trend and the indicator's historical performance.

Risks classified as High and Critical must be addressed through **Action Plans** aimed at lowering their classification, and such actions must be initiated within 60 days of the formalization of the respective plan. Structural plans for mitigating High and Critical **Risk** issues that depend on unavailable resources, highly complex IT projects, or organizational change may be granted extended deadlines, subject to the recommendation of the Vice President of the responsible division and approval by the Statutory Audit Committee. In this case, temporary compensatory controls must be implemented within 60 days, pending the completion of the final **Action Plans**.

TOTVS accepts the **Risks** when the company decides to maintain its current level of exposure without implementing new mitigation measures. This decision must comply with the approval authorities set forth below:

<table>
<tr><th rowspan="2">Risk Rating</th><th colspan="3">Risk assumption authority – TOTVS</th></tr>
<tr><th>Recommendation</th><th>Approval of Acceptance</th><th>Report/Data</th></tr>
<tr><td>Critical</td><td rowspan="2">Chief Executive Officer and Statutory Audit Committee</td><td rowspan="2">Board of Directors</td><td rowspan="2">-</td></tr>
<tr><td>High</td></tr>
<tr><td>Medium</td><td>Vice-president responsible for risk</td><td>Chief Executive Officer</td><td>Statutory Audit Committee</td></tr>
<tr><td>Low</td><td rowspan="2">Director or head responsible for risk</td><td rowspan="2">Vice-president responsible for risk</td><td rowspan="2">Chief Executive Officer</td></tr>
<tr><td>Very Low</td></tr>
</table>

5.1.2.5. Monitoring and Reporting

Proper **Risk** monitoring aims to ensure the effectiveness of the measures taken and timely communication to stakeholders, and is based on the following pillars:

- Ongoing monitoring of the Company's **Internal Control** environment through **Risk** mapping and controls;
- Implementation and monitoring of **Risk** response measures (**Action Plans** and/or controls), the effectiveness of which is tracked by the responsible departments with support from the Internal Controls, Risk, and Compliance department, which is responsible for reporting the consolidated status to TOTVS's Statutory Audit Committee; and
- Establishment and monitoring of **Key Risk Indicators (KRIs)**, defined by the departments responsible for **Risks** in conjunction with the Internal Controls, Risk, and Compliance department. KRIs support the assessment of risk levels **Probability** and **Impact** and the identification of the need for additional **Action Plans**, with the aim of keeping risks at levels deemed acceptable by TOTVS. The **KRIs** should be used by the **Risk Owners** to aid in decision-making and to strengthen the **Culture of Risk Management**.

Any extension of deadlines for the completion of **Action Plans** must be preceded by a formal justification from the responsible department and reported to the Statutory Audit Committee. In the case of **Risks** classified as High and Critical, the Statutory Audit Committee must inform the TOTVS Board of Directors of the reasons for the delay and the new estimated completion date for the relevant plans.

5.1.3. Risk Matrix Review and Evaluation Cycle

The **Risk Matrix** must be reviewed annually by the Internal Controls, Risk, and Compliance department, in accordance with the analysis criteria set forth in this policy, evaluated by the Vice Presidents and the Chief Executive Officer, and submitted for recommendation by the Statutory Audit Committee and for approval by the Board of Directors.

The **Risks** identified in the new **Matrix** must be addressed through **Action Plans** submitted to the Statutory Audit Committee, and their status regarding completion and analysis of changes in the **Risks** within the **Matrix** must be monitored on a quarterly basis The Internal Controls, Risk, and Compliance department is responsible for verifying the implementation of these **Action Plans**.

The Internal Controls, Risk, and Compliance department must also periodically report to the Statutory Audit Committee and the Board of Directors on the progress of the **Action Plans**, the **Key Risk Indicators (KRIs)** calculated, and the level of **Risk Exposure**. Presentations and reports must be included in the annual agenda of the Statutory Audit Committee and the Board of Directors, in accordance with the schedule established for each fiscal year.

5.2. Internal Controls

The internal control framework must be evaluated periodically to assess the effectiveness of existing **Internal Controls** and potential impacts arising from changes in the internal and/or external environment, taking into account: (i) the Company's strategic objectives; (ii) the composition and nature of the accounting accounts; (iii) the possibility of losses resulting from errors and fraud; and (iv) the complexity of transactions in the accounting accounts.

This document is the property of TOTVS. All rights reserved. ©
This document is the property of TOTVS. All rights reserved. ©

5.2.1. Stages of Internal Control Management

The Internal Controls, Risk, and Compliance department must map processes and controls, perform design tests ("walkthroughs"), and conduct effectiveness tests ("Control Tests") to confirm its understanding of the mapped processes and to verify that the controls are implemented and functioning properly.

Controls that are missing or deemed inadequate for mitigating the identified **Risks** are reported to the responsible departments so they can develop **Action Plans** aimed at reducing **Risk Exposure** and improving the control environment.

Once these steps have been completed, those responsible for the processes must conduct an annual Control Self-Assessment (Internal Controls Self-Assessment) in the system used by TOTVS and, where applicable, identify any new risks detected in their processes or activities.

The entire process of mapping and reviewing controls, along with the respective results, is reported to TOTVS's Statutory Audit Committee.

5.3. Compliance

5.3.1. Integrity Program

The **Integrity Program** aims to ensure that all **Employees** are familiar with and comply with applicable laws and regulations, as well as TOTVS's guidelines and rules of conduct, as well as ensuring that the **Third Parties** with whom the Company does business share the ethical principles adopted by TOTVS.

Every year, the Internal Controls, Risks and Compliance Department assesses the activities of each of the **Integrity Program** pillars with the goal of identifying improvements in its processes. This assessment is conducted by monitoring the program's results and indicators reported to the governing bodies during the previous cycle.

The TOTVS **Integrity Program** is structured around five pillars, as described below:

5.3.1.1. Integrity Culture

The purpose of this pillar is to strengthen and promote a culture that aligns with TOTVS's standards of ethics and integrity, through the ongoing engagement and support of TOTVS's senior management and key leaders.

5.3.1.2. Risk Assessment

This pillar aims to identify and assess the main **Risks** from an anti-corruption/**Compliance** perspective to which TOTVS is exposed, as well as measure their **Impacts** and recommend mitigation measures, taking into account compliance with applicable anti-corruption legislation and the conduct guidelines established in the Code of Ethics and Conduct and in the other Standards of the **Integrity Program**.

Compliance risks are reassessed annually by the Internal Controls, Risk, and Compliance department to monitor risks from the previous cycle and to identify and address any new risks that may have been identified.

5.3.1.3. Code of Ethics and Conduct, Policies and Procedures

The purpose of this pillar is to establish and formalize the internal guidelines, rules, and procedures that must be followed by **Employees** and **Third Parties** under the **Integrity Program**, thereby providing a framework for the implementation and/or optimization of integrity mechanisms and controls.

5.3.1.4. Communication and Training

The Communication and Training pillar aims to raise awareness and facilitate the development of a **Risk Management Culture**, as well as to ensure that **Employees** understand the guidelines, rules, and responsibilities they must adhere to under the TOTVS **Integrity Program**.

The Internal Controls, Risk, and Compliance department must develop and implement the Annual Communication and Training Plan, taking into account: (i) the relevance of the topics in light of the guidelines set forth in the Code of Ethics and Conduct and other regulatory documents; (ii) the target audience; (iii) frequency and available communication channels; and (iv) the need to reinforce topics identified in the history of events or questions related to the topic, if applicable.

The Annual Communication and Training Plan must be submitted for review and approval by the Statutory Audit Committee and the Board of Directors, the bodies responsible for overseeing the plan's implementation through reports from the Internal Controls, Risk, and Compliance department.

5.3.1.5. Detection and Remediation

This pillar aims to identify instances of improper or illegal conduct, fraud, or any other violations of applicable laws and regulations and TOTVS's Policies, as well as to ensure that such conduct is stopped and that disciplinary and/or corrective measures are taken, using as its primary tool an independent ("**Ethics and Conduct Channel**") for receiving and handling reports, available to internal and external stakeholders by calling **0800 721 5966** in Brazil and **+55 11 3232 0766** for other locations, or through the website: **https://www.canalconfidencial.com.br/totvs/.**

The **Ethics and Conduct Channel** is managed by the Internal Controls, Risks and Compliance Department, whose primary responsibilities is to (i) receive complaints for investigation by the responsible areas, according to the nature of the reports; (ii) investigate reports of bad conduct; and (iii) report the received complaints to the Ethics and Conduct Committee and other governance bodies as appropriate.

Cases of misconduct are reviewed by the TOTVS Ethics and Conduct Committee, and the Internal Controls, Risk, and Compliance department operates with functional independence and has access to the Committee's meetings, investigation data, and discussions regarding the management of consequences.

6. Consequence Management

In the event of non-compliance with this Policy or the other documents comprising the **Internal Regulatory Framework** and applicable laws and regulations, measures will be taken to address the resulting labor, civil, Criminal, and Administrative consequences that may apply to those responsible for the violations, including the possibility of termination for cause and termination of the contract for just cause in the case of franchisees and any **Third Parties** with whom there is a contractual relationship.

7.Assignments

Board of Directors

- Approve the Risk Management, Internal Controls and Compliance Policy;
- Approve TOTVS's strategic objectives, **Risk** management and **Internal Controls** methodology, and **Integrity Program**;
- Determine the appetite and **Risk Tolerance** levels proposed by the Board of Directors and recommended by the Statutory Audit Committee;
- Annually approve the **Priority Risk Matrix**, taking into account the respective management actions adopted and their results, as well as the **Key Risk Indicators (KRIs)** to be monitored;
- Approve the public information documentation regarding the **Risk** management model and the transparency of information provided to internal and external stakeholders;
- Ensure that adequate resources are available for the effective operation of the **Integrity Program** and guarantee the autonomy of the Internal Controls, Risk, and Compliance department;
- Approve the annual communication and training plan prepared by the Internal Controls, Risk, and Compliance department;
- Review and deliberate on the recommendations of the Statutory Audit Committee regarding the results of Risk Management, Internal Controls, and Compliance, as well as those of the **Integrity Program**; and
- Approve High and Critical **Risk** taking.

Statutory Audit Committee

- Review this Policy and any revisions thereto and submit a recommendation to the Board of Directors regarding its approval;
- Assist the Executive Board in defining the guidelines and methodology for managing **Risks** and **Internal Controls**, as well as the metrics for measuring **Risk Tolerance** and **Risk Appetite**, and submit its recommendation for approval to the Board of Directors;
- Evaluate risk management efforts and the development of the **Priority Risk Matrix**, and present its recommendations to the Board of Directors;
- Assess and recommend to the Board of Directors the establishment of risk appetite and **Risk Tolerance** levels;
- Monitor and periodically evaluate the results of control tests, the **Action Plans** for risk mitigation, and the **Key Risk Indicators (KRIs)** identified, reporting any deviations and incidents deemed relevant to the Board of Directors;
- Discuss and approve the **Annual Compliance Schedule**;
- Evaluate and monitor the **Action Plans** resulting from the audit of the **Integrity Program**;
- Report periodically to the Board of Directors any serious cases of misconduct related to this Policy, as well as any disciplinary measures taken; and
- Make recommendations to the Board of Directors regarding High and Critical **Risk** taking.

Ethics and Conduct Committee

- Monitor and evaluate the reports on the findings and investigations of complaints received through the TOTVS Ethics and Conduct Channel; and
- To determine the validity and severity of complaints regarding violations of the Code of Ethics and Conduct, applicable laws, and/or other internal TOTVS policies, and to recommend to the CEO the appropriate disciplinary action for cases received through the Ethics and Conduct Channel.

Board of Directors and Other Boards

- Conduct business practices that comply with applicable laws and regulations and with the **Internal Regulatory Framework**;
- Support the implementation of the **Integrity Program** and demonstrate commitment to it;
- Manage the **Risks** under their responsibility and assist in the development of controls and mitigation measures; and
- Ensure that TOTVS's code of conduct is communicated to and understood by partners, franchisees, distributors, customers, and other **Third Parties**.

Internal Controls, Risks and Compliance

- Propose amendments and submit this Policy for approval;
- Develop, implement, manage, and disseminate the **Risk** management methodology and the **Integrity Program**;
- Monitor and report on the **Action Plans** and the **Key Risk Indicators (KRIs)** defined for managing **Risks**;
- Raise awareness among managers and other **Employees** regarding the importance of **Risk Management**, **Internal Controls**, and the **Integrity Program**;
- Conduct annual **Internal Controls** in accordance with this policy;
- Act independently and autonomously to ensure impartiality in all activities, and report to the Chief Executive Officer and the Statutory Audit Committee if anything compromises their independence;
- Share with Internal Audit any information and/or facts that are the subject of an internal investigation;
- Manage the activities of the **Ethics and Conduct Channel** and report complaints to the Ethics Committee and other applicable governance bodies; and
- Report on **Risk Matrix** and the results of **Integrity Program** to the Statutory Executive Board, the Statutory Audit Committee, and the Board of Directors.

Internal Audit

- Assess the integrity of information, legal compliance, and the effectiveness of controls, ensuring the protection of assets and the alignment of processes with TOTVS's strategic and governance objectives;

- Assess the effectiveness of the organization's **Risk** management processes and mitigation plans;
- When prompted, investigate complaints received through the **Ethics and Conduct Channel** or by any other means;
- Share, if requested, with the Internal Controls, Risk, and Compliance department any nonconformities identified during the audit; and
- Ensure functional independence and technical objectivity, acting free from external interference and reporting any limitations on its autonomy directly to the Statutory Audit Committee.

Human Relations

- Promote and ensure that the principles of the **Integrity Program** are embedded in TOTVS's organizational culture.

Legal Board

- Advise TOTVS on regulations issued by regulatory agencies and on legislative changes at the federal, state, and municipal levels;
- Report any occurrence of an act constituting an administrative, civil, or criminal offense to the Executive Board and the Board of Directors of TOTVS; and
- Support the Internal Controls, Risks and Compliance area in the interpretation of applicable anti-corruption laws.

Risk Owners/Business and Operational Units

- Continuously identify and document the **Risks** under their management;
- Conduct an annual **Control Self Assessment** of the processes under your responsibility;
- Notify the Internal Controls, Risk, and Compliance department of any new **Risks** identified and any changes to your business processes;
- Implement, calculate, and periodically report the **Key Risk Indicators (KRIs)** to the Internal Controls, Risk, and Compliance department; and
- Implement and execute controls and **Action Plans** in your processes, ensuring that they are effective and result in reducing the level of **Risk Exposure** to acceptable levels.

Other functions

All **Employees**, regardless of their position, have the following responsibilities:

- Comply with the Internal Normative Structure, the applicable legislation and regulations;
- Use the Ethics and Conduct Channel to report any violation or suspected violation of applicable laws or regulations, or noncompliance with the Internal Regulatory Framework; and
- Present all information and/or corporate documents that they possess when requested (i) by the Internal Audit department, (ii) by the Internal Controls, Risk and Compliance department, or (iii) by the Ethics and Conduct Committee, in the scope of the internal investigation.

8. Approvals

Name / Title	Description
Marcos Corradi Executive Manager of Internal Controls, Risks and Compliance	Development and review
Patricia Thomazelli Legal Officer	Review
Gilsomar Maia Sebastião Vice President of Administration and Finance and Director of Investor Relations	Review
Dennis Herszkowicz CEO	Review
Statutory Audit Committee	Recommendation
Board of Directors	Approval