RISK MANAGEMENT POLICY

VERSION 1.0

TABLE OF CONTENTS

1. Definitions

CI&T ("Company"): all references to CI&T include CI&T Inc, Cayman, as well as all of its subsidiaries.

Risk: Possibility of the occurrence of an event or uncertainty that could affect the achievement of the company's objectives.

Inherent Risk: It is the level of risk present in a process or activity without considering the control measures that may be in place. Inherent risk represents the original exposure to risk.

Risk Appetite: Level of exposure to loss that the company is willing to accept.

Risk Management: Process to identify, evaluate and manage potential adverse or inherent events that may impact the achievement of the company's objectives and the performance of its business.

Action Plans: Set of actions that aim to create, correct or improve the functioning of the company's processes, systems and/or strategies, as well as mitigate the causes of risks.

Key Risk Indicator (KRI): Metric that monitors and identifies potential risks that could affect an organization's objectives, anticipating them, providing warning signs that allow proactive actions to mitigate them before they materialize.

Residual Risk: It is the level of risk that remains after implementing mitigation plans.

COSO ERM (Enterprise Risk Management Integrated Framework): Structure developed by the organization COSO - Committee of Sponsoring Organizations of the Treadway Commission, which establishes an internationally recognized Risk Management methodology.

COSO® : Committee of Sponsoring Organizations of the Treadway Commission. It is a private organization created in the USA in 1985 to prevent and prevent fraud in the company's internal procedures and processes. It publishes models for Internal Controls and Risk Management that are considered a reference by the SEC and globally by governance entities.

ICFR ou Internal Control Over Financial Report: Set of processes and practices implemented by an entity to ensure the accuracy, reliability and compliance of financial information.

PCAOB: Public Company Accounting Oversight Board. It is the entity created by SOX to regulate independent audit activity. Subordinated to the SEC, the PCAOB prevents misconduct and failures in independent external audit work, through a permanent inspection program.

SEC: Abbreviation for U.S. Securities and Exchange Commission. It is the regulatory agency responsible for taking care of the United States capital markets. Similar to what the CVM does in Brazil. CI&T is subject to SEC rules.

SOX or Sarbanes-Oxley Act: The Sarbanes-Oxley Act or SOX (Sarbanes-Oxley Act) is an American law of July 30, 2002 that applies to all companies listed on the SEC (Securities and Exchange Commission), whether companies classified as Foreign (which is the case CI&T) or Domestic. The objective of the law is to protect shareholders, requiring corporate governance measures and improvement of internal financial controls.

2. Objective

Risk management is a process of CI&T that strengthens corporate governance.

Risk management is the responsibility of all people, as they act in the execution of control activities, process management and, directly or indirectly, in the treatment of risks to achieve strategic and operational objectives.

CI&T's risk management model, aims to establish bases for continuous assessment and monitoring of risks that affect the business, ways of mitigating and communicating occurrences in a clear and objective manner with all people involved, in addition to improving CI&T's Internal Controls environment.

The main objective of Risk Management is the sustainability of the business, the promotion of a transparent environment, the reliability of information and the effectiveness of the internal control environment.

The objective of this policy is to establish the main guidelines and responsibilities related to risk management, in order to identify, evaluate and monitor the risks inherent to CI&T

and its sector of activity, which may affect the achievement of its objectives and the performance of its business.

3. Applicability

It applies to CI&T and its subsidiaries, as well as to all collaborators, managers, directors, partners and members of the Board of Directors and Committees. In particular, the teams in the areas of Risks, Internal Controls, Internal Audit and Compliance.

4. Directives

4.1 Integrated Risk Management

The Risk Management model adopted by CI&T is based on the COSO ERM methodology. This model is the basis for applying the Management of all Risks from different categories (strategic, operational, compliance and financial) and can be adapted in certain contexts.

It is considered a mopart integrated as it provides for application to different types of risk and it is possible to integrate the actions of different risk management functions and areas responsible for risk governance.

4.2 Corporate Risk Assessment

Corporate risk assessment is a process adopted by CI&T to map potential risks, events and measure possible losses, as well as opportunities generated by them. This process is developed considering all areas of the company and the business panorama.

The objective of corporate risk assessment is to map the risks relevant to the business, based on strategic objectives, so that it is possible to manage them effectively. In addition to classifying risks in relation to their impact and probability, it allows has CI&T prioritize your efforts and investments in actions aimed at risks and controls according to their criticality and relevance.

The stages of the Corporate Risk Assessment process are described below:

4.2.1 Identify Risks and Assessment the Control Environment

This involves identifying the set of events, external or internal, that can impact the organization's strategic objectives through document analysis and interviews with CI&T areas to understand the control environment related to each risk and verification of mitigating actions. existing to minimize their exposure.

4.2.2 Classify Corporate Risks

The risks that this policy envisages being managed may fall into different categories, such as:

4.2.2.1 Strategic Risks

Strategic risks are associated with Senior Management's decision-making and can generate a substantial loss in the company's economic value and even business discontinuation.

In the Strategic pillar, we can highlight the following topics to be evaluated: Planning and Resource Allocation, Governance Structure, Innovation, Communication with the Market, Mergers and Acquisitions, among others. In the strategic vision, risks are also considered from an ESG perspective, such as: incidents involving the environment, climate impacts, human rights such as discrimination, health and safety.

4.2.2.2 Operational Risks

These are risks arising from failures in processes and controls in the company's operations and support areas, which harm or make it impossible to carry out its activities. Operational risks generally result in inefficiency, total or partial interruption of activities, which may have a negative impact on reputation in the market, in addition to the potential for generating contractual and regulatory liabilities.

In the Operational pillar, we can highlight the following topics to be evaluated: Human Resources, Commercial, Purchasing, including Supplier Management.

Technology risks are also in this pillar and we can highlight the following items in the assessment: Adequacy of internal systems to the company's needs, cybersecurity incidents, data integrity and management, failure in logical access to systems, data leaks, among others.

4.2.2.3 Risks of Compliance

Compliance Risks refer to the possibility of an organization incurring legal, financial or reputational sanctions due to non-compliance with applicable laws, regulations, standards and internal policies, as well as failure to follow established ethical standards. The risks are mapped based on the topics of the Compliance Program and include regulatory aspects, conflicts of interest, corruption, money laundering, related parties, offering and receiving gifts, among others.

4.2.2.4 Financial Risks

Financial risks refer to the possibility of losses resulting from CI&T's financial operations and transactions, which may result from inefficiencies in the management of cash flow, liquidity, debts, capture and application of financial resources, exchange rate variations and failures in disclosure of financial information.

4.2.3 Assess Risks in terms of their Impact and Probability

To optimize resources and efforts, the risks to be managed must be prioritized according to their relevance to CI&T, resulting from the assessment of impact and probability according to pre-established criteria, which are detailed in the internal operational procedure for Corporate Risk Management.

4.3 Implement Action Plans to Risk Mitigation

As a result of identifying risks and evaluating the control environment, the applicability of discussing and aligning with those responsible must be verified. the recommendation of mitigating and/or corrective actions to reduce exposure to risks. Actions must be prioritized and implemented considering the company's exposure to risk.

4.4 Monitor Identified Risks and Action Plans

The Corporate Risk Assessment must be carried out annually or whenever a area implement or modify controls that affect the probability or impact of a risk occurring. With this exposure review, the residual risk.
Additionally, the action plans defined to mitigate risks must be monitored periodically, considering the deadline for implementing the activities agreed with the people responsible for updating the data and monitoring the associated risks.
The impact and probability classification parameters regarding the materialization of risks must also be reviewed annually based on the results of the Corporate Risk Assessment.

4.4.1 KRI Definition and Monitorings (*Key Risk Indicators*)

The definition and monitoring through Key Risk Indicators contribute to identifying the need to implement actions to reduce exposure or the amount of occurrence of the risk materialization must be carried out periodically together with the responsible areas, according to the nature of the indicator/risk, identifying the need for corrective and mitigating actions in a timely manner.

Preparation of the KRIs report (*Key Risk Indicators*) must occur quarterly and be structured with a view to communicating results to the areas involved, and has the following main objectives:

- Alert Management about risks that need attention;
- Issue alerts when corrective actions are necessary;
- Alert the Risk Management and Internal Controls function, in addition to Internal Audit, about areas of the company that require a review of internal controls.

5. Responsibilities

The responsibilities for the CI&T's Risk Management process are structured according to the descriptions below:

5.1 Board of Directors

- Approve the Risk Management Policy and its future revisions;
- Evaluate the matrix corporate risks and the controls implemented for discussion and strategic decision making.
- Approve to Matrix company risk

5.2 Audit Committee

The Audit Committee, an advisory body to the Board of Directors, is responsible for supervising the adequacy and effectiveness of processes related to risk management, through the following activities:

- Evaluate the adequacy of the operational structure of the Risk Management area in order to guarantee the effectiveness of the risk management policy;
- Review and discuss with management significant risks or exposures and evaluate the measures management has taken to minimize these risks;
- Define the risk appetite that the company is willing to accept in its activities to achieve its strategic objectives.
- Evaluate and monitor the matrix of CI&T risks, as well as the effectiveness and sufficiency of mitigating controlsories and propose improvements;
- Propose recommendations for improvements to the areas of internal control and risk management and monitor their implementation in order to eliminate or mitigate any relevant deficiencies identified.

5.3 Risk Management

The Risk Management area is responsible for developing and assisting in the implementation of this policy, methodologies and tools for risk management. The Risk Management function within the scope of this Policy is responsible for:

- Annually review and update the Risk Assessment and Mapping Corporate;
- Develop, review and keep risk Probability and Impact criteria updated;
- Validate and communicate the results of the Corporate Risk Assessment with the people involved;
- Assist in the deployment of recommendations resulting from the Corporate Risk Assessment into processes and action plans with the responsible people, aiming to reduce the level of exposure to risks;
- Prepare a report with the results of the Corporate Risk Assessment and communicate them to the Board of Directors, through the Audit Committee;
- Monitor, evaluate and consolidate data related to KRIs within the areas;
- Promote integrated communication and disseminate CI&T's risk management culture;
- Review this policy annually, or whenever necessary.

5.4 Internal Controls

The internal controls area is responsible for assisting in defining, monitoring and testing the effectiveness of controls carried out by areas of the company.

The Internal Controls function within the scope of this Policy is responsible for:

- Establish the processes, management methodology and monitoring of CI&T's internal controls, considering in addition to controls related to SOX requirements, the critical controls arising from corporate risks operational and strategic areas;
- Assist areas with action plans and improvement of processes and controls to reduce the level of exposure to risks;
- Monitor the execution and implementation of action plans in the areas;
- Work on evaluating the effectiveness of internal controls, identifying and providing visibility on points of control deficiency;
- Contribute to meeting the requirements of SOX, PCAOB and SEC legislation, cconducting the process of Assessment or Certification of the Internal Control Environment over Financial Results or ICFR.

5.5 Compliance Area

The Compliance area is responsible for, within the scope of this Policy:

- Ensure the application of the CI&T Code of Ethics and Conduct;
- Ensure the smooth functioning of the CI&T Compliance Program;
- Carry out risk management related to the Compliance Program, that is, based on the 8 pillars of the program (Code of Ethics and Conduct and Policies, Communication and Training, Reporting Channel, Internal Investigations, Due Diligence, Senior Management Support, Management of Compliance and Internal Audit Risks and Internal Controls);
- Report the results of Compliance risk management to the Audit Committee and the Board responsible for the Compliance Program;
- Assist the Risks and Internal Controls Function and the Board in assessing Compliance Risks, and coordinate process improvements to mitigate them.

5.6 Internal Audit

- Provide independent opinions to the Board of Directors, through the Audit Committee, on the risk management process, the effectiveness of internal controls and corporate governance;
- Submit to the Audit Committee an internal audit plan, covering the most relevant areas, processes, activities and risks of CI&T, for review and approval;
- Reevaluate the Plan periodically regarding its adequacy to possible changes in business, risks and operations, among other aspects;
- Carry out work aimed at analyzing the quality and applicability of internal controls at CI&T, compliance with policies and procedures and compliance with the CI&T Code of Ethics and Conduct;
- Report significant risk exposures and control deficiencies to the Audit Committee;
- Communicate internal audit results the Audit Committee and related areas;
- Conduct monitoring and reporting activities of corrective action plans undertaken as a result of observations made in assessment work.

5.7 Directors of production areas and support areas

Each The Board is responsible for managing and monitoring risks related to its area of performance, which can compromise corporate objectives and goals. The Board of Directors is responsible, within the scope of this Policy:

- Promote the integration of risk management with the processes of the areas under its responsibility;
- Define Action Plans and people responsible for their implementation within their area context, provide the guidelines and allocate necessary resources for the implementation of this plan;

- Report on risks and action plans for the Audit Committee and/or Board of Directors when requested;
- Monitor the risks under its responsibility;
- Align with the areas of of Risks and Internal Controls, actions to implement applicable corrective and mitigating actions to reduce risk exposure;
- Signal the need to review the probability and impact assessment of risks under its responsibility when the control environment is modified or risk materialization events occur;
- Contribute to corporate risk assessments and reviews.

5.8 Management, leadership and collaborators in production areas and support areas

Risk management is the responsibility of all people, as they act in the execution of control activities, process management and, directly or indirectly, in the treatment of risks to achieve strategic and operational objectives. They are responsible for:

- Evaluate, validate, manage and monitor the risks under your responsibility;
- Implement actions in accordance with the Action Plan defined to mitigate risks in the areas involved;
- Inform the Risk Management area and Board of Directors about changes in mapped risks and new risks identified;
- Execute controls and processes to mitigate risks;
- Measure indicators for risk monitoring;
- Maintain action plans, forms and corporate Risk Management tools updated.

6. Document control

Version	Date	Description	Author
1.0	JAN/2023	Creation	ERM Team (Risk Management)
1.0	DEC/2024	Revision	Compliance, ESG, Information Security, Internal Controls and Internal Audit Teams, Stanley

1.0	DEC/2024	Audit Committee Review	Audit Committee Members
1.0	DEC/2024	Final approval	Board of Directors