1. PURPOSE

Establishing principles, concepts, guidelines, and responsibilities in the Risk Management of Companhia Brasileira de Distribuição and its subsidiaries that are not publicly traded companies (collectively, "GPA") regarding the identification, review, and assessment of risks that may affect their strategic goals and the effective creation and protection of value for GPA.

Defining, from inherent risks, exposure control and monitoring devices, incorporating the risk vision into strategic decision-making in compliance with the applicable legal requirements, best practices and applicable market methodologies.

2. SCOPE

Applicable to all macro processes and business operations of Companhia Brasileira de Distribuição and its subsidiaries that are not publicly traded companies.

3. TERMS, EXPRESSIONS, AND DEFINITIONS

Risk Appetite: this means the degree of risk the Company is willing to accept in accordance with the risk/return ratio, to achieve its goals within the limits set by the senior management.

Capacity: the resources available for the Company to meet its strategic plan, such as financial capital resources, technologies, processes and people, among others.

COAUD: Company's Audit Committee.

COMEX: Company's Executive Committee.

Company: Companhia Brasileira de Distribuição.

Risk Consequences: these are aggravating factors in the outcomes and impacts of an Event that could positively or negatively affect the Company's ability to achieve its goals.

DIREX: Company's Board of Officers.

Event: an occurrence or set of events, the impact of which can affect GPA's results, whether positively or negatively.

Risk Management: a set of coordinated and structured activities aiming at aligning the Risk Appetite with the strategic decision-making cycle in order to optimize the results set forth in the strategic planning and the effective creation and protection of GPA's value.

GPA: Companhia Brasileira de Distribuição and its subsidiaries that are not publicly traded companies.

Impact: these are aggravating factors or consequences if the risk materializes, which can be categorized into Financial and Reputation.

Key Performance Indicator (KPI): metrics used to measure and monitor process performance and results, which can also be used for risk monitoring.

Probability: it is the possibility of the Risk to materialize, and can be reported qualitatively, quantitatively and by frequency.

Risk: factors and/or events that may have negative impacts, compromising the Company's ability to achieve its strategic goals and the effective creation and protection of GPA's value.

Inherent Risk: degree of risk intrinsic to the operation of the business or activity, without considering the performance of controls and direct actions able to reduce its exposure; also called gross risk.

Prioritized risks: a list of risks deliberately set by Senior Management that describes exposure levels that may enhance high impacts to the business, the management of which should be prioritized in a structured manner.

Residual Risk: degree of risk already considering all controls and actions identified to reduce exposure.

Tolerance: the limits of acceptable variation in the performance against the achievement of business goals.

4. RESPONSIBLE AREAS, ROLES AND RESPONSIBILITIES

We describe herein below all interested parties that are within the context and life cycle of the Risk Management process, with their corresponding responsibilities:

Function	Responsibilities
Board of Directors	• Establishing general Risk guidelines aligned with the business context and the strategic planning cycle; • Establishing acceptable Risk Appetite limits under GPA's Capacity and Tolerance; • Evaluating, deliberating, and approving the strategic and Prioritized risk matrix aligned with the Risk Appetite; • Influencing and sponsoring the monitoring of Priority Risks, within the management forums; • Influencing and sponsoring the risk culture within GPA; • Assessing, annually, the sufficiency of the structure and the budget of the Internal Auditors for the performance of their duty; • Revising and approving the general definitions of Risk Management strategies; • Approving the risk policy, its evolution and future reviews.
COAUD	• Following the activities of the Internal Auditors and the area of internal controls of GPA. • Evaluating and monitoring the exposure Risks of GPA. • Proposing, to eligible forums, definitions and guidelines that will compose the Risk Management model within GPA; • Monitoring and supporting the Risk Management process in defining Priority Risks aligned with the business context and the Board of Directors' guidelines; • Supervising Risk Management activities by complying with legal laws, policies, rules and internal procedures of GPA; • Evaluating and monitoring the Priority Risks found by the revisions of the Risk Management areas, reporting it to the Board of Directors and assisting it to assess action plans and recommendations;

	• Evaluating, approving, and monitoring how Prioritized Risks are addressed and monitored. • Evaluating, approving and recommending to the administration the correction or improvement of the internal policies of GPA. • Evaluating the company's quarterly information, interim statements and financial statements.
Human Resources and Corporate Governance Committee Sustainability and Diversity Committee	• Preparing the planning and ensuring that the Risk Management is actually put into operation, considering all dimensions of the structure set, encompassing strategic, tactical, and operative activities of GPA; • Assisting the Board of Directors in applying the Risk Management methodology in GPA; • Supporting the Board of Directors in defining both the Risk Appetite and GPA's priority risks; • Supporting GPA in reviewing and approving of the Risk Management strategy; • Assisting the Audit Committee and the Board of Directors on risk exposure levels; • Assessing the effectiveness of GPA's Risk Management process; • Identifying the risks arising from GPA's strategic and policy changes under the approval by the Board of Directors.
COMEX/DIREX	• Promoting the integration and risk culture in GPA and in management cycles and strategic planning; • Ensuring the implementation of an efficient Risk Management model, aligned with business purposes and business goals. Applying the general guidelines set by the Board of Directors to assign the acceptable Risk Appetite level for GPA; • Monitoring all Risks managed to ensure the effectiveness of control measures; • Taking part in the validation rituals and risk prioritization of GPA. • Following up KPIs and Priority Risk mitigation strategies; • Assessing and monitoring how business risks are addressed, aligned with the performance of strategic planning; • Assessing, on a timely basis, the effectiveness and applicability of risk policy guidelines; • Assessing and supporting the suitability of the structure for the management process, considering human, financial and technological resources.
Risk Management Director	• Setting and improving the Risk Management methodology, which shall be integrated and aligned with the value chain over the entire GPA; • Managing GPA's Risk Management process cycle, covering all business units; • Ensuring the information flow management within all business units aligned with the concepts, methodology, and deadlines set for each Risk Management cycle; • Supporting business units in the risk identification, assessment, treatment, and monitoring cycle to assist them in reducing risk exposure levels;

	• Managing the Prioritized Risk matrix, reporting their status and exposure levels to the key management forums; • Supporting business areas in identifying and assessing the impact of Risks. • Following up the implementation of the action plans by the responsible area and report possible delays and/or increment of Risks to GPA.
Risk Owner	• Identifying, ranking, and managing the Risks of the corresponding areas according to mitigation strategies, together with the Risk Management area; • Appointing the professional who will answer as facilitator in Risk Management with the Risk Management area; • Ensuring the implementation of action plans and monitoring of KPIs; • Reporting exposure levels, action plans, and indicators describing Residual Risk status to governance and management forums.
Facilitator / Person in charge	• Having technical knowledge of the processes in which Risks are inserted; • Being the responsible person for updating the mapping information and Risk treatment of his/her business unit; • Keep information updated in a timely manner, respecting the planning calendar of the Risk Management cycle; • Monitoring the status of action plans with those ones responsible for implementing control measures.
Internal Auditors	• Measuring the quality and effectiveness of the company's processes related to Risk Management, control and governance; • Identifying and pointing out opportunities for improving Internal Control and Risk Management processes; • Auditing information and controls connected to KPIs developed and monitored by functional areas; • Reporting periodically to COAUD and its audited clients the results of independent, unbiased, and timely assessments of the effectiveness of Risk Management in GPA.
Associates	• Ensuring that Risk Management is put into operation, becoming part of the process of identification, assessment and measurement, implementing preventive and corrective actions; • Taking part in training sessions able to allow the conscious dissemination of the Risk Management culture.
External Auditors	• Assessing the quality of internal controls focused on prepare financial statements, reporting to GPA the weaknesses on those controls if found it.

Table 1: Roles and Responsibilities

5. SPECIFIC GUIDELINES

Our general guidelines are our commitment to GPA's value proposition, aligned with our code of ethics and conduct so that we can create a Risk Management culture that reaches all our associates.

Risk Management is part of GPA's Audit and Corporate Governance process and is an integral part of the decision-making process, contributing to the performance of its strategy. Risks are identified and addressed to ensure compliance with the goals set out in the strategic planning.

For that purpose, the Risk Management structure considers the joint action of the corporate governance and management areas, according to the concept of the 4 lines of defense as described in *table 2* below:

1st line	2nd line	3rd line	4th line
- This line is composed of Operations Management, represented by the boards of executive officers, managers, and other associates of the business units that operate in day-to-day operations and tasks. - They must manage performance and Risks taken in compliance with the policy. - They implement controls, action plans, and timely report information connected to Risk Management.	- This line is composed by areas of control and supporting functions, represented by the Risk Management Director, that may require the advice by the internal areas of GPA responsible for *Compliance* matters, Internal Controls and Information Security. - They should guide, monitor, and assess adherence to all standards and policies set, in addition to support the first line of defense in achieving GPA's purposes. - They should make it easier, disseminate, and monitor Risk Management practices and assist in identifying Risks according to the set Risk Appetite.	- This line is in charge of assurance functions, represented by the Internal Audit, responsible for conducting audits or reviews of Risk Management and Internal Control practices, as well as governance effectiveness, identifying problems and opportunities for improvement with independence, objectivity, and authority for recommendations.	- This line represents the functions of the Independent External Audit, entity that has as mission the evaluation of the quality of the internal controls used to elaborate the financial statements. This line also represents a line of defense, since the Independent External Audit has to report to the Company all the liabilities in such internal controls, may they find any.

Table 1: Lines of Defense

5.1. RISK MANAGEMENT PROCESS

The GPA Risk Management process was determined based on the guidelines of COSO - *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) and also on the ISO 31000:2018 standard - Principles and Guidelines for Risk Management.

Such process life cycle is made up of 7 subsequent and dependent steps, which we perform once a year as shown in *Figure 1*.

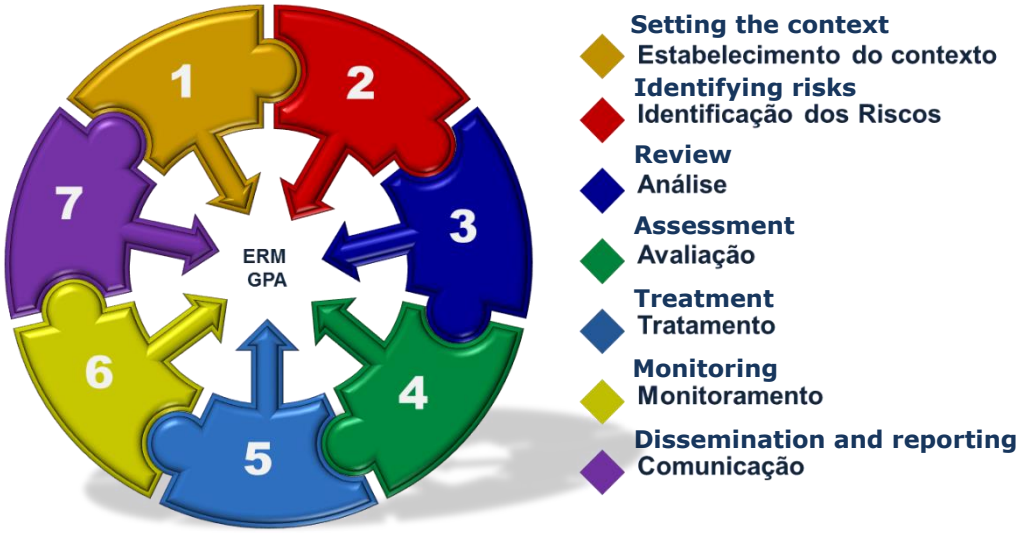

Figure 1: steps of GPA's Risk Management Process

5.2. STAGES OF THE PROCESS

Stage 1 - Setting the Context:

Understanding the business scenario and context considering factors connected to the short- and long-term strategic planning of GPA aligned with the environment in which such goals are inserted.

This is a critical step to ensure that the Risk Management process is aligned with the GPA management and strategic planning cycles to align with its acceptable Risk Appetite levels.

It consists of an annual cycle of executive alignments with process owners and the senior management to compose a benchmark that will provide support to the next steps of identifying risks that are most aligned with the business context.

To determine the scenarios that should support this stage we considered two influencing factors, namely:

- **External Factors**: Economical, Environmental, Political and Social.
- **Internal Factors**: Infrastructure, Human Resources, Processes and Technologies.

Stage 2 - Risk Identification:

The Risk identification approach is top-down, starting with interviews with key executives of GPA, considering the main processes they are responsible for.

The product generated at this stage is a comprehensive list of event-based Risks that could identify vulnerabilities and threats able to jeopardize the achievement of GPA's strategic goals.

At this stage the owner and the responsible for every single risk identified must be determined, as well as a description that will guide the next steps of the mapping.

Stage 3 - Review:

It is performed a more detailed review of the identified risks, including important attributes for clarity and qualitative and quantitative support to generate variables able to holistically rate the universe of risks for us to act more assertively in their prioritization.

It is determined, among other aspects, their causes or risk factors and their effects, rating their aggravating factors so that we can generate a comprehensive and relevant list of risks for further mapping.

Information is gathered to obtain data able to describe the likelihood and Impacts of risks, thus generating a qualitative matrix to describe in an executive way the universe of risks based on their ranks, as described herein below in *Figure 2*.

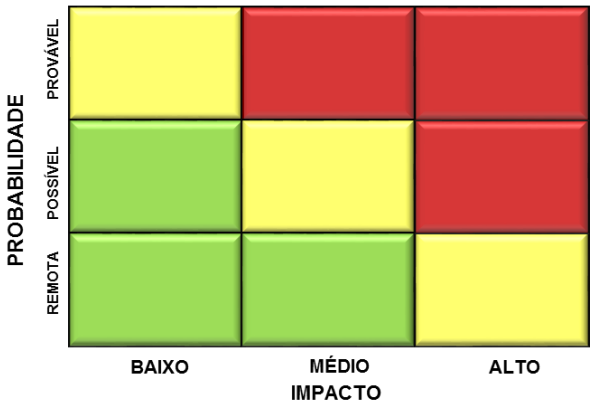

Figure 2: Qualitative Risk Matrix

The risks are classified within this qualitative matrix, according to the following criteria:

- **High Rating or High Risk (Red)**: they represent a potential threat to GPA's business and there must be priority actions to reduce or eliminate the Risk component.

- **Medium Rating or Medium Risk (Yellow)**: these represent a threat and can be monitored and managed through preventive control measures able to maintain the degree of exposure or Risk acceptance.
- **Low Rating or Low Risk (Green)**: they represent an acceptable threat with minor impacts and no need for continuous monitoring, which can be accepted.

Stage 4 - Assessment:

We assess the Inherent Risks and their potential materialization impacts to achieve GPA's goals.

With the support by the senior management, executive officers, and process leaders, we assess events from the perspective of probability or frequency and impacts. We seek variables to combine qualitative and quantitative assessment methods.

We consider, among others, variables to rank impacts that help in better risk classification, using the high, medium, and low gradient for each variable.

Finally, by combining all the assessment variables, we define the criticality of Risks found that allows us to build a prioritization map, starting from the highest exposure to the lowest exposure Risks.

This map supports GPA to achieve a greater degree of strategic planning alignment, and also an acceptable Risk Appetite level for the Company.

Stage 5 - Treatment:

The Risk treatment stage involves identifying the existing control devices within the process to rate their effectiveness as a preventive measure and as a factor reducing the exposure (Mitigating Factor) that will help to determine the Residual Risk.

For processes that require a greater degree of control effectiveness or that do not have effective mitigation factors, we perform at this stage the implementation of one or more action plans to mitigate risk factors.

For each action plan, we assign responsible persons and implementation schedules to ensure the effectiveness and efficiency of the plans and thereby reduce the level of Residual Risk.

Within this process, we apply alternative Risk responses, as shown in *table 3*:

Suppress	Reduce or Mitigate	Transfer	Accept
Taking actions that change and/or abolish a process or a project, protecting business	Taking control measures to reduce the likelihood and/or impact of a Risk to an acceptable level,	Taking actions that reduce the Likelihood and/or Risk Impact by fully transferring or	No action is taken to affect the Likelihood and/or Impact of the Risk as it is within an

goals from the impacts of this Risk.	according to the Risk Appetite.	sharing a portion of the Risk.	acceptable level of Risk Appetite.

Table 3: Risk response alternatives

Stage 6 - Monitoring:

Consisting of a dynamic and continuous cycle, it is essential to ensure timely, preventive, and reactive actions that help minimize Impacts in case Risks materialize.

Associates involved in each area must have the ability and competence to identify, assess, prioritize, monitor, and manage their Risks, taking into account all changes within the internal and external environment, so that they can achieve the highest degree of control over their processes to achieve their goals as established on Risk Management (*see table 3*).

The Risk monitoring process consists of two main fronts, namely:

- **Action Plans**: these must be carried out by the business units according to the responsibilities determined by the Risk owners, which may vary from monthly, bimonthly, quarterly, semiannually, and even annually, depending on the Risk Management needs.
- **Control measurement**: metrics and indicators are connected to Risk factors and preventive measurement factors that are identified during the Risk treatment stage, according to the control devices, determining acceptable limits that inductively describe whether the indicators point out trends or deviations that could make the risks to materialize, thus enabling triggers for the business units to take actions to reverse events and, consequently, their impacts.

Stage 6 - Dissemination and reporting:

Regularly an alignment ritual is done to aim at spreading the Risk Management culture through workshop, training sessions, and/or rendering of account rituals with risk owners and the key GPA management forums such as the Board of Directors, COAUD.

To fulfill such dissemination and reporting ritual, it is determined a plan that develops communication formats according to the target audience, describing the frequency, the persons involved, and the responsible.

5.3. RISK CLASSIFICATION

We adopt 4 risk classifications within the process, namely:

- **Strategic**: Risks that affect GPA's strategy or strategic goals. They are connected to scenarios of uncertainties and/or opportunities and are a priority focus of senior management.
- **Operations**: Risks arising from some inadequacy or failure to manage internal processes, people, or technologies that may hinder or prevent goals to be achieved.
- **External**: Risks coming from external factors or it is not under GPA controls.

- **Corporative Social Responsibilities (CSR):** risks related to ESG, approaching environmental, social and governance that affects GPA.

6. PENALTIES

Employees who witness non-compliance with any of the above rules have the duty to report such violation to the Ombudsman Channel. In addition, failure to comply with the rules and guidelines imposed in this document may be considered a serious misconduct, subject to disciplinary sanctions based on the Management Policy of the Ethics Committee, GPA Code of Ethics and the Policy on Disciplinary Consequences and Sanctions.