WEG GROUP RISK MANAGEMENT POLICY

1. PURPSOSE
Establish an operational and administrative program for risk management and business continuity for the WEG Group, contributing to the achievement of organizational objectives.

2. SCOPE
This policy applies to all WEG Group units in Brazil and abroad, as well as to affiliated and controlled companies.

3. REVIEW CYCLE
The Risk Management Policy must be reviewed every two years or whenever necessary to keep its content up to date. The approving bodies are the Controllership Committee, General Management, and the Board of Directors, taking into consideration the recommendation of the Audit Committee.

4. ROLES AND RESPONSIBILITIES
Risk management should not be treated as the exclusive responsibility of a single area, but rather as a collective commitment embedded in the daily routine of the entire Company. Engagement at all levels—strategic, tactical, and operational—is essential for risk management to be effective and integrated into business decisions.

Below are the main roles and responsibilities of the parties involved in the risk management process:

4.1. BOARD OF DIRECTORS (CA)
- Approve the Risk Management Policy and its amendments;
- Deliberate on the general guidelines for the Company's risk management;
- Establish the risk appetite and the guidelines to be observed in the risk management process;
- Approve the response strategy for identified risks

4.2. AUDIT COMMITTEE
- Assess and monitor the Company's risk management system;
- Track risk exposures and, when necessary, request information to support the assessment of exposures and proposed mitigation activities;
- Support the Board of Directors on matters related to risk assessment;
- Evaluate policies and procedures related to the identification and management of risks within the WEG Group.

4.3. EXECUTIVE COMMITTEE
- Approve and monitor the implementation of the Risk Management Policy;
- Monitor the Company's main risks;
- Provide guidance and make decisions whenever necessary in light of identified risks.

4.4. INSURANCE AND RISK DEPARTMENT
- Act as an integrator and facilitator for business units on topics related to risk management;
- Be responsible for the Company's consolidated risk register and for implementing and maintaining the Risk Management Policy;
- Establish and keep current the documentation, information, and methodology for risk management;
- Monitor, analyze, and report changes in risk criticality;
- Support and monitor the Company's risk identification and assessment process;
- Assist Risk Owners in managing, controlling, and defining risk response plans;
- Update and review the risk mapping with the Company's executives whenever there are changes in strategic planning or material events;
- Promote a risk management culture within the organization and strengthen the 1st and 2nd Lines of Defense, as defined in item 5.

4.5. RISK OWNERS
- Assess and validate the risks under their responsibility;

- Manage the risks and, together with the areas involved, implement the actions necessary for their mitigation;
- Notify the Insurance and Risk Department whenever there are changes in the probability, impact, or characteristics of the risk;
- Inform the Insurance and Risk Department about unmapped risks or risks not previously addressed;
- Complete and keep up to date the risk management forms and tools.

5. RISK GOVERNANCE

WEG adopts the three lines of defense concept as described below:

1st Line of Defense: Responsible for identifying, assessing, defining internal controls, and treating risks. These are the business areas whose manager serves as the Risk Owner. This manager is responsible for monitoring and executing the approved action plans.

2nd Line of Defense: Areas responsible for developing and implementing this policy, for the methodologies for risk assessment and mapping, and for supporting the business areas in executing action plans, always aligned with strategic planning. They also promote a risk management culture within the Company and monitor adherence to the Company's policies and procedures. The second line is composed of, but not limited to, the areas of Insurance and Risks, Internal Controls, Certification, Compliance, and Standards Audit.

3rd Line of Defense: A role performed by Internal Audit, which conducts independent and objective evaluation and advisory activities regarding the adequacy and effectiveness of governance and risk management..

6. RISK MANAGEMENT PROCESS

The risk management process at WEG is structured in a cyclical and continuous manner, covering the stages of risk identification, assessment, response, monitoring, and communication. The activities are formalized in procedure WPS-28756.

- **Identification**: detection of events that may impact the Company's strategic, operational, financial, and compliance objectives. Risks are classified into six categories listed below:

1) External: Risks originating from external processes/actions, beyond WEG's control, that may cause direct or indirect damage.

2) Strategic: The ability to anticipate, protect against, or adapt to changes that may affect WEG's strategic directions.

3) Financial: WEG's ability to raise or preserve financial resources.

4) People: WEG's ability to attract, develop, retain, and have at its disposal human resources, or those related to employee health and safety.

5) Compliance & Governance: WEG's ability to conduct its activities in accordance with policies, internal control rules, laws, and regulations, as well as to protect itself against fraud.

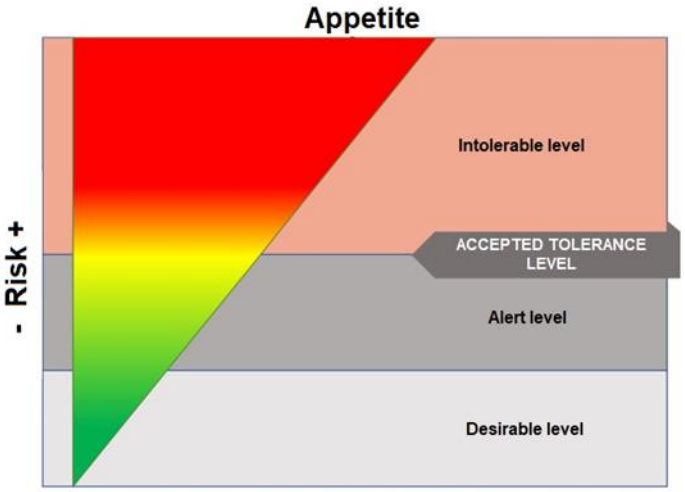
6) Operational: The ability to use available resources effectively and efficiently, ensuring the proper functioning of the operations chain and the correct operation of its Information Technology systems and infrastructure.

- **Assessment:** analysis of the frequency and severity of each identified risk, allowing classification and prioritization.
- **Response**: definition and implementation of strategies to treat risks, such as mitigation, acceptance, transfer, or elimination.
- **Monitoring:** continuous tracking of the evolution of risks and the effectiveness of implemented actions, as well as identifying changes in the internal and external environment.
- **Communication:** structured and timely sharing of risk information among stakeholders, ensuring alignment, informed decision-making, and engagement at all levels of the organization.

The risk update process must occur at least every two years, under the coordination of the Insurance and Risk Department, ensuring adherence to changes in the Company's internal and external environment.

7. RISK APPETITE

Risk Appetite establishes the limits the Company is willing to accept in order to achieve its objectives. Composed of the “Desirable, Alert, and Intolerable” risk levels, the appetite sets the boundaries within which the Board expects Management to operate and serves as the basis for prioritizing and deciding the appropriate treatment (response).



Exposure Level	Direction
Extreme	Risk above the approved tolerance limit; the area must create an action plan for treatment. These risks are presented annually to the Executive Board and the Board of Directors.
High	
Medium	Risk close to the tolerance limit; the area must create an action plan for treatment and monitoring.
Low	Risk below the accepted tolerance limit; no follow-up required.

8. BUSINESS CONTINUITY MANAGEMENT (BCM) OF THE WEG GROUP

BCM aims to prepare WEG to:

a) Respond quickly to disruptive event scenarios (natural or man-made, accidental or intentional) demonstrating command and control as a response to these events.

b) Recover and restore critical operations after the occurrence of a disaster.

BCM will evaluate the business discontinuity scenarios identified as per item 8.1.

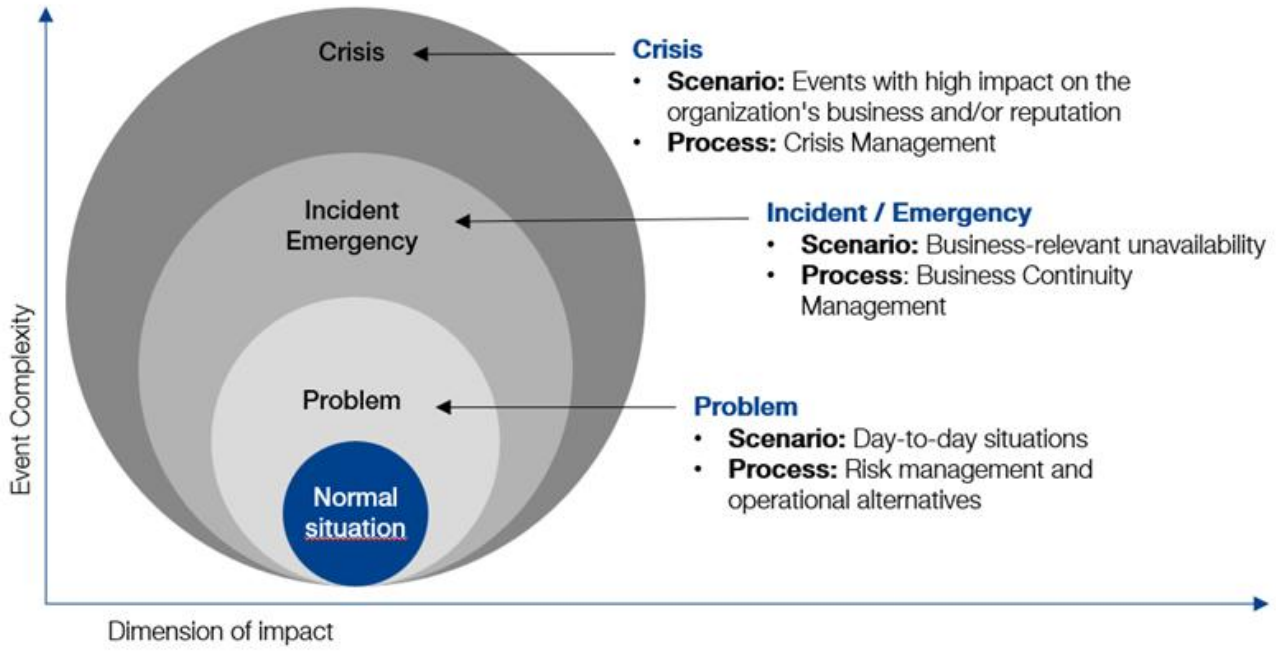
8.1 DISCONTINUITY EVENTS

The focus of BCM is on responding to events “b” and “c” as outlined below:

a) Problem: Everyday situation that must be monitored and treated, as it has the potential to generate significant impacts on the operation. In these cases, the risks must be monitored in the risk mapping in accordance with the established action plans.

b) Incident / Emergency: Events that deviate from standard operations and may cause operational interruption for some period, must be supported by the BCM process (e.g., fire, weather events, strikes, blockades, etc.).

c) Crisis: Event that has the potential to damage the company’s image or the relationships with stakeholders (e.g., major accidents, recalls, and others).



8.2 BUSINESS CONTINUITY PLAN (BCP)

The BCP is a document prepared by the Insurance and Risk Department in conjunction with each business unit to assess interruption scenarios considering the macro flow of the unit's processes and to determine the roles and responsibilities of the areas involved in recovery activities. This document must be reviewed every 2 years and recorded in the unit's board meeting.

8.3 FUNCTIONAL DECISION GROUPS

These are the people who will be called in a scenario of discontinuity. Contact information will be included in the BCP, and responsibilities are described as follows:

a) Crisis Management Group – Responsible for approving communication actions with stakeholders in conjunction with the executive board, supervising the activities of the operational group, and managing contingency scenarios and supporting the decision-making process of the Executive Board. This group consists of:
Finance and IR Director;
HR Director;
Corporate Legal and Compliance Manager.

b) Operational Group – Response group for a crisis/emergency event convened by the director responsible for the activity/operation, whose role is to provide support and physical or technological infrastructure, food, transportation, access to facilities, recovery activities, site functionality restoration, etc.

c) Support and Communication Areas – Responsible for contacting the press, external entities, insurance companies and suppliers, as well to ensure the proper dissemination of information to internal areas.

8.4 POST-CRISIS

After the resumption of activities following an interruption event, the Insurance and Risk Department will coordinate an evaluation of lessons learned and improvement opportunities by observing:

I. Costs involved in the event;
II. IRP recovery and review roadmaps;
III. Corrective actions to prevent similar cases;
IV. Communication actions with interest groups;
V. Lessons learned (what worked and what didn't).

This information must be included in a report to be approved by the Executive Committee.

9. STANDARDS AND REGULATIONS

For this policy, the following standards were followed:

- ISO 22301:2013: Societal Security – Business Continuity Management System;
- ISO 31000:2009: Risk Management – Principles and Guidelines;
- NFPA 1600 – 2019: Standard on Continuity, Emergency, and Crisis Management;
- COSO 2017: Enterprise Risk Management — Integrating with Strategy and Performance.

10. BUSINESS CONTINUITY PLAN (BCP)

The business continuity plan and the incident response plan are defined in WPR-58999.