Risk Management Policy

DCA 034/2019	Rev.: 03-31/07/2019	POL-0009-G	PUBLIC

Purpose: To establish guidelines and guidance for the integrated management of potential risks which Vale System entities are exposed.

Scope:

- This policy applies to Vale, its wholly owned (100%) subsidiaries and shall be reproduced to its direct and indirect, subsidiaries in Brazil and in other countries, always respecting these companies' constitutional documents and the applicable laws. Adoption of this policy is encouraged in other entities in which Vale has a participation interest in Brazil and in other countries. This group of entities, for the purposes of this Policy, is referred to as "Vale System".

References:

- POL-0001-G - Code of Ethical Conduct
- POL-0016-G - Anti-Corruption Policy
- POL-0025-G – Sanctions Compliance Policy

Principles and Guidelines:

The risk management should:

- Support strategic planning, budget and sustainability of Vale System business.
- Strengthen capital structure and asset management of Vale System, by including concepts and assumptions of management based on the risk in perspective on operations and maintenance of assets and logistics modes.
- Strengthen Vale's governance practices, based on the lines of defense model.
- Consider concepts of ISO 31000, ISO 55000 and COSO-ERM as references for risk management. For Operational Safety, adopt the RBPS (Risk Based Process Safety) as the operational safety management system.
- Measure and monitor Vale's System potential risks, on a consolidated basis, considering the effect of diversification, when applicable, of its whole business.
- Establish a specialized structure for specific and independent performance, as 2nd Line of Defense Specialist, in the assessment of potential operational risks, including geotechnical risks.
- Assess the impact of new investments, acquisitions and divestitures on Vale's System risk map and risk tolerance.

Risk Concept:

- Risk is the effect of uncertainty on the organizational objectives that manifests itself in many ways, with potential impact on all business dimensions.
- The business risk management focuses on the relevant potential risks that, if occurs, could impact people, communities, environment, operational continuity, reputation and the achievement of the company's overall business objectives.

Integrated Risk Map:

- The Integrated Risk Map is a non-exhaustive tool, that contains the set of potential risks proposed by Executive Board and approved by the Board of Directors, which needs to be assessed for its applicability on operational, commercial, projects, support and administrative areas in Vale sites at different geographies, being distributed in categories, which include, but are not limited to, strategic, financial, operational, cybernetic and compliance.
- Periodically, at least once a year or when requested, the risks should be evaluated and validated by Vale's Board of Directors, by recommendation of the Executive Board, and may be maintained, reviewed, excluded or included in the Integrated Risk Map.

Risk Matrix:

- The Risk Matrix allows comparisons among potential risk events, allowing prioritization for preventive risk treatment. The Matrix is defined and filled in with each potential risk event, according to the combination of impact severity and probability.
- The Severity and Probability tables in the "Risk Management" chapter of Planning, Development and Management Standard (NFN-0001) are tools that help to assess risk events in perspective and, prioritize their preventive treatment and aim to minimize the subjectivities and standardize the evaluations, making them comparable and enabling the compliance with applicable legal requirements for operational and business scenarios.
- The severity table is used to assess the progressive severity of impacts in different dimensions including Financial, Social and Human Rights, Reputational, Environment, Occupational Health and Safety and Process Safety.
- The Probability table is used to statistically estimate the theoretical probability of occurrence of a risk, as long as it has a rationale that can be audited. In other situations, the risk owner (1st Line of Defense) should evaluate the probability of occurrence of a risk event.
- Very Critical severity events, which may lead to a permanent business disruption, should be monitored regardless of any probability criteria.

Risk Tolerance:

- The Executive Board is responsible for proposing the risk tolerance for each quadrant of the Risk Matrix to Vale's Board of Directors, establishing the quadrants corresponding to risks with unacceptable level and the quadrants corresponding to continuous monitoring level. For these levels, semi-quantitative or quantitative risk studies should be performed to confirm the frequency of the scenario.
- The Executive Board should promote the reduction or elimination of risks classified at unacceptable level in the Risk Matrix by: (i) additional mitigation and prevention actions; (ii) transfer or sharing, in total or in part, the risk; or (iii) risk rejection, for example through a temporary or definitive closure of a plant or shutdown of an activity.
- For risks at continuous monitoring level in the Risk Matrix, the risk owner (1st Line of Defense) must ensure the effectiveness of controls and the timeliness of action plans.
- For other levels in the Risk Matrix, the risk owner (1st Line of Defense) must control and prevent through critical control elements (barriers), manage through the safety process system and/or monitor through proactive and reactive indicators, and, request support from the 2nd Line of Expert Defense whenever consider necessary.

Risk Management Governance Structure:

- Vale has an integrated Risk Management Governance flow, which is based on lines of defense model, representing how revaluations are periodically carried out to ensure the alignment between strategic decisions, performance, definition and monitoring of risk tolerance limits approved by the Board of Directors, by proposing of Executive Board.

General Governance

- The Board of Directors has, for its advisory, committees that, in general, are responsible for monitoring the scope and the effectiveness of business risk management in accordance with the guidelines established by Vale's Board of Directors and to act preventively in addressing the risks presented at committee meetings.
- The Business Risks Executive Committees, established by Vale's Board of Directors, are divided into four (4) committees with different scope of action: (i) Operational Risks, (ii) Geotechnical Risks, (iii) Strategic, Financial and Cybernetics Risks and (iv) Compliance Risks.
- The Business Risks Executive Committees should:
  - Promote the culture of business risk management in the company.
  - Support the 1st Line of Defense on additional requests for human, financial and other resources to proper manage and prevent potential risks, and, in particular, to the reduce or eliminate risks classified at unacceptable level and for the effectiveness controls and timeliness of action plans for the risks classified at continuous monitoring level.

- Support Vale's Executive Board to monitor operational, geotechnical, strategic, financial cyber and compliance risks and issue preventive recommendations regarding potential risks presented at the meetings of these committees.
- Recommend reviews on risk management principles and tools, aimed to continuous process improvement.
- Evaluate and suggest, when necessary, changes on the strategy of business risk management for subsequent approval by the Executive Board.
- Provide the Executive Board with a consolidated macro view of Vale System's potential risk exposure in Operational, Strategic, Financial, Cybernetics or Compliance dimensions, as appropriate, and assist in the development of the Multi-Annual Risk Management Plan.
- Propose, when necessary, consequences management for any eventual non-compliance with action plans recommended by these committees and by the Executive Board, regarding to risks.

Vale's Executive Board

- Monitor business risks management systematically.
- Promote the culture of business risks in the organization and the empowerment of 1st and 2nd Lines of Defense.
- Support the organization, including the risk owner (1st Line of Defense) and the 2nd Line of Defense, with human, financial or any kind of resources, through decisions under their authority, in order to reduce or eliminate the risks at unacceptable level and to ensure that the risks at continuous monitoring level have effective controls and action plans.
- Annually propose to the Board of Directors the Multi Annual Risk Management Plan, including the consolidated requirement for sustaining investments and other resources necessary to mitigate potential risks.

1st Line of Defense

Consist on the risk owners, who are directly responsible for keeping the risks within the tolerance limits defined by Vale, and the process executors of operational, commercial, project, support and administrative areas. They hold the primary responsibility and directly manage the risks, identifying, evaluating, treating, preventing and monitoring their risks in an integrated way.

Responsibilities of the 1st Line of Defense:

- Implement and execute effective preventive and mitigation controls, ensure appropriate definition and execution of action plans and establish corrective actions for the continuous improvement of risk management.
- Continuously assess the applicability of risks in the Integrated Risk Map to the activities and geographies under their responsibility.
- Recommend adjustments in the Integrated Risk Map when consider necessary and ensure the record of the risks, in case they do not fit in with the existing risks presented in the map.
- Ensure the compliance with external regulations, policies and internal standards.
- Operate and maintain the integrity and the reliability of assets, should develop, implement and ensure the performance of assets from operations, projects, support and administrative activities. Must immediately stop the asset(s) operation in case of critical deviations or in the event of a partial or complete unavailability of critical control elements that move the risk to unacceptable level.
- Proactively implement and execute, any mitigation or elimination actions that consider necessary, to transfer or to share or to reject risks at unacceptable level.
- Ensure, for risks at continuous monitoring level, the effectiveness of controls and the timeliness of action plans.
- When consider necessary, request additional support to push forward the preventive treatment of risks under their responsibility, and submit the request to the Business Risks Executive Committee(s) for proper addressing.
- In the event of imminent risks, the 1st Line of Defense must immediately and proactively take the corrective actions, which consider appropriate, with no need to obtain prior authorizations. Subsequently if any support above the established authority limits is required, should submit the request directly to the Executive Board.
- In the event that the imminent risk is at unacceptable level as well, the 1st Line of Defense must take over for themselves higher authority limits to approve emergency measures. Subsequently, such measures, if adopted, shall be submitted for ratification by the competent authority.
- Establish and implement Crisis Management protocols and Business Continuity plans for the risk events under their responsibility, classified with severity Very Critical and Critical, and, for other risks whenever applicable. For risks

with impacts Very Critical and Critical, drills should be performed in order to verify the efficiency and effectiveness of the Crisis Management protocols. The frequency of the drills should be defined by the 1st line of defense according to the criticality, considering local rules and specific legislation.
• Comply with the guidelines, minimum technical and management standards defined by the 2nd lines of defense.
• Certificate (sign off), annually or on demand, that the risks with severity Very Critical and Critical related to the processes under their responsibility are duly identified, assessed and recorded in Vale's risk management system. Must certify that controls have been implemented, are properly executed and monitored in accordance with established guidelines. In addition, has to ensure that action plans address weaknesses and are properly monitored regarding the implementation deadline.

2nd Line of Defense

Enterprise Risk Management (ERM) - Business Risks Integrated Management

Regarding business risks management, the Enterprise Risk Management (ERM) structure has the following responsibilities:

- Develop and implement policies, methodologies, processes and infrastructure for integrated risk management.
- Support the work of the 1st Line of Defense by providing training and tools for risk management and risk prevention.
- Support and promote the exchange of knowledge and information in order to disseminate the risk management and risk prevention culture in the organization.
- Support and monitor the compliance with business risks governance model.
- Support external disclosure of official business risks management information.
- Report information about the Integrated Risk Map to Vale's Business Risks Executive Committee(s) meetings, considering the status of controls and business risk action plans.
- Consolidate the decisions of Business Risks Executive Committees for submission to the Executive Board, as well as follow up the accomplishment of recommendations, being responsibility of the 2nd Lines of Defense Specialists to assess their technical effectiveness, when applicable.
- Coordinate the certification (sign off) of risks with severity Very Critical and Critical to be carried out, annually or on demand, by the 1st Line of Defense.

The Enterprise Risk Management (ERM) area will report to the Finance and Investor Relations Executive Director.

Safety and Operational Excellence – Operational Risks Management

For the purposes of this Policy, operational risk management, under the responsibility of Safety and Operational Excellence department, corresponds to the performance as 2nd Line of Defense Specialist on potential risks with impacts on the Health, Occupational Safety and Process Safety dimensions, as well as on potential geotechnical risks, whose responsibilities are:

• Act as technical responsible for the definition of standards and rules for management of Occupational Safety, industrial and geotechnical processes.
• Act as the normative and inspector area for the critical assets management process.
• Keep an integrated management system that ensures consistence in application of standards and operational management good practices.

2nd Lines of Defense Specialist

In addition to the Safety and Operational Excellence department, which is the 2nd Line of Defense for Operational Risks, there are areas such as the Environment, Corporate Integrity and Information Security that should also act as 2nd Line of Defense Specialist for the respective potential risks.

All 2nd Lines of Defense Specialist have the following attributions:

• Act within the corporate guidelines for risk management and risk prevention established by the Enterprise Risk Management (ERM) area.
• Define methodologies, minimum technical, technologic and management standards, as well as risks and assets reliability indicators to be mandatorily adopted by the 1st Line of Defense.
• Provide tools and training to the 1st Line of Defense, supporting their improvement in the management and prevention of specific risks.
• Define the prioritization of critical control elements and test their integrity.
• Support the identification of deviations and risks and issue recommendations, give support to the deployment of the model and standards to manage and prevent risks and assets.
• Inspect the implementation of standards and indicators and evaluate the execution of operational, commercial, project, support and administrative areas (1st Line of Defense), with independence and transparency.
• Establish a mandatory integrated operational management system.
• Evaluate the effectiveness of controls related to relevant potential risks executed by the 1st Line of Defense. In case of critical deviation(s), has the power to define immediate actions to be implemented by the 1st Line of Defense, and may decide to stop the operation of the asset(s).
• Address relevant potential risks to specific Executive Committees, if preventive actions decisions, which require additional support, are necessary.

The definition of which areas in the organization will perform as 2nd Line of Defense Specialist is delegated to Vale's Executive Board.

3rd Line of Defense

- The 3rd line of defense is composed of areas with total independence from the administration, that is, the Internal Audit and the Ethics and Conduct Office which perform, observing their respective scopes, evaluations, inspections, by the execution of controls test and investigations of allegations, providing exempt assurance, including on the effectiveness of risk management, internal controls and compliance.

General Rules

- Vale’s Board of Directors delegates to the Vale’s Executive Board the approval to deploy this Policy into rules and responsibilities to manage and control the risks, in order to avoid the occurrence of unwanted accidents of MUE (Major Unwanted Event).
- This Policy shall be reviewed periodically, at least once in every three (3) years or on demand.