Risk Management Policy

DCA 025/2021	Rev.: 06- 15/03/2021	POL-0009-G	PUBLIC

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

Scope:

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

References:

- POL-0001-G – Code of Conduct
- POL-0005-G – Human Rights Policy
- POL-0012-G – Climate Change Policy
- POL-0016-G – Anti-Corruption Policy
- POL-0019-G – Sustainability Policy
- POL-0025-G – Sanctions Compliance Policy
- POL-0032-G – Water and Water Resources Policy
- POL-0033-G – Policy for provision of audit services by the independent auditor
- POL-0035-G – Vale Management Model Policy - Vale Production System - "VPS"
- POL-0036-G – Diversity and Inclusion Policy
- POL-0037-G – Policy for Dam Safety and Geotechnical Mining Structures
- POL-0040-G – Mining and Metallurgical Waste Management Policy

Principles and Guidelines:

The risk management should:
- Support strategic planning, budget, and sustainability of the Vale System's business.
- Strengthen the Vale System's capital structure and asset management, introducing management concepts and criteria based on the risks of the operation, the assets maintenance, and the 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 System's potential risks on a consolidated basis, considering the effects of diversification, when applicable, of its whole business.
- Establish a specialized structure for dedicated and independent performance, as the 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 System risk map and risk tolerance.

Risk Concept:

- Risk is the effect of uncertainty on the organizational objectives, that manifests in many ways with potential impact on all business dimensions.
- In Vale System entities, risks are categorized as Business Risks, Corporate Process Risks and Operational Process Risks. The classification of the risk event in each of these categories is based on the Severity Table, the Executive Board must propose the classification limits to the Board of Directors, when necessary or upon demand by the Board itself. Risks must be properly registered in the Risk Management System, by the 1st Line of Defense, according to its category.

- Business Risks are relevant potential risks that, in the event of an occurrence, may impact people, communities, the environment, operational continuity, reputation and the achievement of the company's general business objectives and strategy.
- Corporate Process Risks are those related to possible deviations in transactional corporate processes, with no possibility of significant impacts on the company's strategic objectives. In addition, such risks include the functions of Marketing and Sales, Assets (management of fixed assets), Human Resources, Finance, Information Technology, Supplies, Legal and Tax, not exhaustively.
- The Corporate Process risk should be classified as a business risk when it has an impact on the "Reputational" and / or "Financial" dimensions at a Moderate or greater severity level.
- The identified risks whose impact assessment by the risk owner does not have any dimension above Low and Very Low should not be considered as Business Risk, consequently with no obligation to be registered in the Business Risk Management System.
- The Operational Processes Risks emanate from the company's production process. They are usually related to physical integrity failure of assets and process equipment and are characterized by unplanned or uncontrolled release of hazardous material or energy.
- Operational Process risk should be classified as Business Risk when it has an impact on the "People" and / or "Environment" dimensions at a Very Critical severity level.

Integrated Risk Map:

- The Integrated Risk Map is a non-exhaustive tool that contains the set of potential risks themes proposed by the Executive Board and approved by the Board of Directors, which needs to be assessed and monitored in all Vale units in the different geographies of its operational, commercial, project, support and administrative areas. Such risk themes are set out in the Integrated Risk Map into categories, including, but not limited to, People, Sustainability, Institutional Relations and Reputation, Strategic, Cyber, Financial, Planning and Operational Continuity, Geotechnics and Compliance.
- Periodically, at least once a year or when requested, the themes should be evaluated and validated by Vale's Board of Directors, as recommended by the Executive Board, and may be maintained, reviewed, deleted, or included in the Integrated Risk Map.

Risk Matrix:

- The Risk Matrix contains the risk classification based on the combination of two factors: Probability and Severity of events. This combined analysis establishes a risk priority scale, with each event being classified as Very High, High, Medium, or Low priority. This method allows comparisons among potential risk events, allowing prioritization for preventive risk treatment.
- The Severity and Probability tables are tools that help assess risks and prioritize its preventive treatment. These documents aim to minimize the subjectivities and standardize the evaluations, making them comparable and enabling the compliance with applicable legal requirements for business risk scenarios, operational process risks and corporate process risks.
- The Severity table is used to assess the progressive severity of impacts in different dimensions including People, Environment, Social and Human Rights, Reputational and Financial.
- The Probability table is used to statistically estimate the theoretical probability of occurrence of a risk, as long as a rationale that can be audited is used. In other situations, the risk owner (1st Line of Defense) should evaluate the probability of the risk event's occurrence, being necessary to define the rationale used.
- The 2nd Line of Defense Specialist is responsible for approving the prevention and mitigation plan proposed by the 1st Line of Defense for all events with a Very Critical severity level arising from HIRA, regardless of any probability criteria. It is important to emphasize that HIRA (Hazard Identification Risk Assessment) is the official process to identify and classify operational and geotechnical risks.
- It is the 1st Line of Defense responsibility, through indicators and controls, to ensure that the action plans established to prevent or mitigate risks, whatever its classification, are being implemented within the deadline, prioritizing actions that lead to reduction of severity.

- POL-00037 (Safety Policy for Dams and Geotechnical Mining Structures) describes other processes for assessing and mitigating geotechnical risks (as well as its approval levels) that are additional to HIRA, such as Engineer of Records (EoR).
- The Executive Board is responsible for proposing to Vale's Board of Directors the Risk Matrix and the Severity Table.
- The approval of the Probability Table(s) is delegated to the Executive Board.

Risk Tolerance Matrix:

- The Risk Tolerance Matrix establishes the strategy and governance to be followed in response to risks, based on the event classification in the Risk Matrix.
- The Executive Board is responsible for proposing to Vale's Board of Directors the risk tolerance limit for each priority level of the Risk Matrix, establishing the strategy and governance in response to risks.
- The Executive Board should provide human, financial, and other resources, by approval within their authority limits, the support required by the 1st and 2nd Lines of Defense to reduce or eliminate risks classified at the "Mandatory Risk Level Reduction" in the Risk Matrix and allow that the risks classified at the "Continuous Monitoring" level have effective controls and action plans, through:
  - (i) additional mitigative and preventive actions;
  - (ii) transferring or sharing, in total or in part, the risk or;
  - (iii) risk elimination, for example, through a temporary or definitive closure of a plant or shutdown of an activity.
- For risks classified as "Continuous Monitoring" in the Risk Tolerance Matrix, the risk owner (1st Line of Defense) must evaluate the effectiveness of controls and the timely execution of action plans aiming at managing risk with regard to its prevention and mitigation.
- For other classification levels of Risk Tolerance Matrix, the risk owner (1st Line of Defense) must control and prevent risks through use of critical control elements (barriers), manage risks through the safety process system and/or monitor risks through proactive and reactive indicators, and request support from the 2nd Line of Defense Specialist whenever deemed necessary.

Risk Management Governance Structure:

- Vale has an integrated Risk Management Governance flow, which is based on the Lines of Defense model, establishing how revaluations are periodically carried out, aiming the alignment between strategic decisions, performance, definition and monitoring of risk tolerance limits approved by the Board of Directors, on the recommendation of the Executive Board.

General Governance:

- The Board of Directors has advisory committees that, as provided for in the Bylaws, which, among other duties, are responsible for overseeing the scope and the effectiveness of business risk management by the Executive Board in accordance with the guidelines established by Vale's Board of Directors.
- The Business Risks Executive Committees, established by Vale's Board of Directors, are divided into five (5) committees with different scope of action: (i) Operational Risks, (ii) Geotechnical Risks, (iii) Strategic, Financial and Cybernetics Risks, (iv) Compliance Risks and (v) Sustainability, Institutional Relations and Reputational Risks. The committees act preventively and have the mission to support Vale's Executive Board in monitoring business risks and in its deliberations according to this policy.
- The Business Risks Executive Committees should:
  - Promote the Business Risk Management culture in the company.
  - Support the 1st Line of Defense on additional requests for human, financial and other resources for the adequate management and prevention of potential risks, and, in particular, to reduce or eliminate risks classified at "Mandatory Risk Level Reduction", in the effectiveness of the controls and timely execution of action plans for the risks classified at continuous monitoring level.
  - Support Vale's Executive Board in monitoring operational, geotechnical, strategic, financial, cyber, compliance, sustainability, institutional relations, reputational, people, planning and operational continuity risks and issue preventive recommendations regarding potential risks presented at the meetings of these committees.
  - Recommend reviews on risk management principles and tools, aiming at the continuous improvement of the process.

- Evaluate and suggest, when necessary, changes on the business risk management strategy for subsequent approval by the Executive Board.
- Provide the Executive Board with a consolidated macro view of the Vale System exposure to potential risks in the categories of the Integrated Risk Map: People, Sustainability, Institutional Relations and Reputation, Strategic, Cyber, Financial, Planning and Operational, Operational Continuity, Geotechnics and Compliance, as appropriate, and assist in the development of the Risk Management Multi-Annual Investments Plan.

Vale's Executive Board:

- Monitor business risks management systematically.
- Promote the business risks culture in the organization and the empowerment of 1st and 2nd Lines of Defense.
- Define which areas of the organization will act as 2nd Line of Defense Specialist.
- Provide human, financial and other resources, by approvals within their authority limits, the support required by the 1st and 2nd Lines of Defense to reduce or eliminate risks classified at "Mandatory Risk Level Reduction" in the Risk Matrix and to allow that the risks classified at the "Continuous Monitoring" level have effective controls and action plans, through:
  - (i) additional mitigative and preventive actions;
  - (ii) transferring or sharing, in total or in part, the risk or;
  - (iii) risk elimination, for example through a temporary or definitive closure of a plant or shutdown of an activity.
- Approve the Probability Table(s), for a minimum period of 3 years.
- Propose the assessment and validation, by Vale's Board of Directors, of the Integrated Risk Map themes and the Risk Management Multi-Annual Investments Plan, considering the consolidated need for current investment, with a minimum annual periodicity.
- Propose to Vale's Board of Directors the revision of the risk management tables and matrices listed below, with a minimum period of 3 years:
  - Severity Table, including the criteria for classifying the risk event in the categories of Business Risk, Corporate Process Risk and Operational Process Risk
  - Risk Matrix
  - Risk Tolerance Matrix for each priority level of the Risk Matrix
  - Strategy and Governance Tables in response to risks

1st Line of Defense:

- The 1st Line of Defense consists of Vale personnel responsible for executing the Company's operational and business processes, they are responsible for registering the risks identified in the entire chain of the operating model; for managing risks; for implementing risk management controls and their respective action plans.
- It consists of the risk owners, who are directly accountable for maintaining risks within the tolerable limits defined at Vale; by the control owners, accountable for the execution of the preventive and mitigative controls assigned to them by the risk owner(s); and by personnel responsible for executing the operational, commercial, project, support services and administrative business processes.
- The 1st Line of Defense must share and provide technical and methodological support regarding the standards and guidelines for safety and risk management established in Vale's operations with contracted suppliers.
- Every business risk identified by the 1st Line of Defense must be attributed to a risk owner, with a minimum position of Manager.

Responsibilities of Risk Owners:

- Operate and maintain the integrity and the reliability of assets, developing and implementing the performance of assets from operations, projects, support, and administrative activities. Must immediately stop the asset(s) operation if critical deviations occur or if complete or partial unavailability of critical control increases the risk to the "Mandatory Risk Level Reduction".
- Proactively implement and execute mitigation or elimination actions deemed appropriate, whether transfer, share or reject risks classified at the "Mandatory Risk Level Reduction".

- Manage risks directly, identifying, assessing, treating, preventing, and monitoring risks consistent with Vale's Integrated Risk Management Process.
- Continuously assess the applicability of risks themes in the Integrated Risk Map to the operations and associated activities under their accountability.
- Recommend adjustments in the Integrated Risk Map when appropriate and register potential risks, including cases where it does not fit with the existing risks themes defined in the Integrated Risk Map.
- Monitor risk compliance in order to meet external regulations, policies and internal standards.
- Ensure the effectiveness of controls and the timely execution of action plans, especially of the risks classified in the "Continuous Monitoring" and "Mandatory Reduction" levels.
- When deemed necessary, to continually improve the preventive or mitigative control of risks, the risk owner should request additional support in the hierarchical line or the 2nd Line of Defense Specialist and guide the risk monitoring with the corresponding Business Risk Executive Committee(s).
- In the event there is an increased likelihood a risk may materialize, the risk owner must immediately and proactively take the preventive and mitigative actions, which he considers appropriate, with no need to obtain prior authorizations. Subsequently, if any support is required, or if ratification is or is believed to be required at higher levels, the request must be forwarded to the corresponding department or function, according to the governance of the response established in the Strategy and Governance in Response to Risks Tables.
- In the event there is an increased likelihood a risk classified at the "Mandatory Risk Level Reduction" may materialize, the risk owner must assume higher decision-making authority to approve the enactment of emergency measures. Subsequently, such measures, if enacted, must be reported to the respective Executive Director and submitted for ratification by the responsible authority according to the Delegation of Authority Policy - (POL-0002-G)
- Establish and implement Crisis Management protocols and Business Continuity plans for all risk events within their responsibility that are classified with Critical or Very Critical severity, and, for other risks when appropriate. For risks with Critical and Very Critical severity, drills should be performed to verify the efficiency and effectiveness of the Crisis Management protocols. The frequency of the drills should be defined by the risk owner according to the risk rating, considering local rules and specific legislation and according to internal normative documents, always following the most restrictive deadline.
- Comply with the technical and management guidelines defined by the 2nd Lines of Defense.
- Periodically monitor risk management indicators to ensure the effectiveness of the controls and action plans associated with the risks within their accountability.
- Evaluate corrective action plans, proposals for continuous improvement of controls and / or implementation of new controls suggested by control owners, aiming at the risk management continuous improvement.
- Follow Vale's budget guidelines to obtain the necessary resources for risk management.
- Certify (sign off), approving in the Risk Management System the formalization of risk and any subsequent associated changes, such as reevaluation of causes, controls and/or other elements.

Responsibilities of Control Owners:
- Manage the preventive and mitigative controls assigned, ensuring the accuracy and timeliness of the information and integrity of the process, in accordance with the applicable legislation, internal policies and standards, and seek to correct the controls, in the event a deficiency is identified.
- Perform or review all control tests, respecting the frequency defined in the control documentation. It is recommended that all evidence of the performance of High and Very High residual risk test should be documented and stored in the Risk Management System, so that the test can be subsequently verified by the 2nd Line of Defense Specialist and / or 3rd Line of Defense.
- Mobilize the risk owner if deficiencies are found in control verification tests, which have an impact on risk prevention or mitigation, especially in the case of critical controls.
- Elaborate and / or associate action plans for controls that do not work or with required implementation, to seek the effectiveness and feasibility for the control to work.
- Monitor the execution and timeliness of action plans related to controls, as well as current investments when associated with the control(s).
- Certify (sign off), approving in the Risk Management System the formalization of the control and any changes on it.

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 the Integrated Business Risk System needed so that business risk management takes place at Vale in a standardized way.
- Support the 1st Line of Defense, providing the methodology, tools, and associated training on the Business Risk Management model.
- Support and promote the exchange of knowledge and information in order to disseminate the risk management and risk prevention culture at Vale.
- Support and monitor compliance with the business risks governance model.
- Support external disclosure of official business risks management information.
- Report the Integrated Risk Map to Vale's Business Risks Executive Committee(s) meetings, considering the status of business risks controls and action plans.
- Consolidate the decisions of the Business Risks Executive Committees for submission to the Executive Board and follow up the status/completion of such recommendations. It is the responsibility of the 2nd Lines of Defense Specialists to assess the technical effectiveness of such recommendations, when applicable.

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 Executive Board, corresponds to the performance as 2nd Line of Defense Specialist on potential risks with impacts on the People dimension, as well as on potential geotechnical risks, whose responsibilities are:

- Act as technical authority responsible for the definition of standards and rules for management of Occupational Safety, Industrial processes, Geotechnical processes, and asset integrity.
- Act as the authority and assure the critical assets[1] management process is established according to the adopted concepts.
- Keep an integrated and regular management system in the application of standards and good operational management practices.
- Monitor and present the risks associated with operational processes with a level of Critical or Very Critical severity, in the forums indicated by the Operational Excellence and Risk Committee.

In addition to the responsibilities described above, the areas from Safety and Operational Excellence Executive Boards have the responsibilities, as follows bellow, from 2nd Lines of Defense Specialist.

2nd Line of Defense Specialist:

In addition to the Safety and Operational Excellence Executive Board, which is the 2nd Line of Defense for Operational Risks, there are areas such as the Environment, Corporate Integrity, Social and Human Rights, not exhaustively, 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 Vale System's Risk Management corporate guidelines.
- 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.
- Define the method and technical selection criteria of critical control.
- Conduct independent checks (assessment of effectiveness) of critical controls, related to relevant potential risks owned by the 1st Line of Defense. In the exercise of their duties, if any deviation is identified in the existing controls

---

[1] As defined in the internal normative documents of the normative area (PNR-000044).

and barriers for risks classified as High and Very High priority, the 2nd Line of Defense has the power to specify immediate actions to be implemented by the 1st Line of Defense, including the authority to stop the operation of the assets, when applicable.

• Act in support of the 1st Line of Defense, by assessing the concepts adopted, verifying whether the risks have mapped controls and whether the barriers implemented are suitable and adequate to the relevant potential risks.

• Support the risks identification, the need to implement additional controls, the identification of non-conformities of existing controls and issue recommendations, provide technical support in the implementation of the model, management standards and risk prevention.

• Assess the implementation of standards and indicators by the operational, commercial, project, support, and administrative areas (1st Line of Defense), with independence and transparency.

• 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 Whistleblowing Channel which perform, observing their respective scopes, evaluations and inspections through the execution of control tests and complaints investigation, providing exempt assurance, including on the effectiveness of risk management and prevention, internal controls, and compliance.

• Monitor and evaluate the effectiveness of the company's key risks management process, as defined by the Board of Directors.

• Evaluate the effectiveness and efficiency of processes, the applicability of VPS, HIRA standards, among others, as well as the compliance with the guidelines related to engineering, maintenance, geotechnics, and Health & Safety areas, by employing a specialized technical team.

• Monitor and evaluate governance, compliance, and internal controls processes, including the effectiveness of the activities of the 1st and 2nd Lines of Defense.

• Consult and provide advisory services, provided they are intended to add value and improve the governance, risk management, and control processes, and the internal auditor does not assume responsibility inherent to the duties of the Process Owners and the 1st and 2nd Lines of Defense.

• Communicate to the responsible management and competent governance bodies about exposure to significant risks and control deficiencies.

General Rules:

• Vale's Board of Directors delegates to the Vale's Executive Board the approval to deploy this Policy into rules and responsibilities directed to risks and controls management, in order to avoid the occurrence of unwanted accidents of MUE (Material Unwanted Event)[2] and / or materialization of potential risks.

• This Policy must be reviewed periodically, at least 1 (once) in every 3 (three) years or on demand.

---

[2] MUE (Material Unwanted Events) is an unwanted event that has the potential to (i) result in multiple fatalities or (ii) extensive and irreversible environmental impact outside the site or loss of operating license. It is a term derived from the methodology HIRA - Hazard Identification and Risk Analysis, used by operational areas to survey operational risks.