Risk Management Policy

PTVI-POL-0009	Rev.: 00-12/12/2025	PUBLIC

REVISION HISTORY/*RIWAYAT REVISI*

Revision Index/ ***Indeks Revisi***	**Subject/*Subyek***	**Technical Area/*Area Teknis***	**Date of Application/*Tanggal Keberlakuan***
00	Risk Management Policy	Enterprise Risk Management/ *Manajemen Risiko Perusahaan*	12 December 2025/*12 Desember 2025*

Approval/ Persetujuan:		**Next review date/ *Tanggal Peninjauan Berikutnya:***
	Bernardus Irmanto President Director/*Presiden Direktur* Date/*Tanggal*:	12 December 2028 (or earlier as applicable)/ *12 Desember 2028 (atau lebih awal jika berlaku*)

Approval Reference/*Referensi Approval*:
Approved by the Board of Commissioners through meeting as stated on the Minutes of Meeting dated 12 December 2025/Disetujui *oleh Dewan Komisaris melalui rapat sebagaimana tercantum dalam Risalah Rapat tertanggal 12 Desember 2025.*

Proposed by/*Diusulkan oleh*:	**Technical Area/ *Area Teknis*:**	**Reviewed by/*Ditinjau oleh*:**		
The Board of Directors/*Dewan Direksi*	**Enterprise Risk Management/ Manajemen Risiko Perusahaan**	**Enterprise Risk Management/ *Manajemen Risiko Perusahaan***	**Legal & Compliance/*Hukum & Kepatuhan***	**Corporate Governance/*Tata Kelola Perusahaan***
Proposal Reference/*Referensi Usulan*: Proposed by the Board of Directors through meeting as stated on the Minutes of Meeting dated 04 November 2025/*Diusulkan oleh Dewan Direksi melalui rapat sebagaimana tercantum dalam Risalah Rapat tertanggal 04 November 2025.*	Batara Indra Digitally signed by Batara Indra DN: cn=Batara Indra, c=ID, o=PTVI, ou=ERM, email=batara.indra@vale.com Date: 2025.12.19 17:28:07 +07'00'	N/A	Digitally signed by Anggun Kara Nataya DN: cn=Anggun Kara Nataya, c=ID, o=PT Vale Indonesia Tbk, ou=Legal Department, email=anggun.kara.nataya@vale.com Date: 2025.12.19 17:32:56 +07'00'	Budi Handoko Budi Handoko cn=Budi Handoko, c=ID, o=PT Vale Indonesia Tbk, email=budi.handoko@vale.com I have reviewed this document 2025.12.22 08:15:44 +07'00'

Risk Management Policy

PTVI-POL-0009	Rev.: 00-04/11/2025	PUBLIC

1. Objective

PT Vale Indonesia Tbk ("**PTVI**") remains steadfast in its commitment to its purpose: to improve lives and transform the future together. Nonetheless, uncertainties whether arising from internal dynamics or external environmental factors may pose challenges to the achievement of business objectives and strategic goals. Recognizing and managing these uncertainties is essential to sustaining PTVI's long-term success and resilience.

To enhance the likelihood of achieving business objectives and to mitigate the impact of unforeseen events, PTVI hereby establishes and maintains a comprehensive risk management framework through this Risk Management Policy (the "Policy"). The integration of risk management into sound governance practices ensures that all strategic business decisions are made with due consideration of both potential opportunities and associated risks. This approach safeguards the profitability, capital, assets and reputation of PTVI.

This Policy sets forth the principles and guidelines for the integrated management of potential risks to which PTVI may be exposed. The institutionalization of Risk Management within PTVI's organizational culture is intended to foster heightened awareness across all levels of the organization. It also aims to cultivate a shared understanding and consistent expectations regarding risk management practices, thereby reinforcing a proactive and resilient approach to risk across the enterprise.

2. Scope

This Policy is applicable across all functions and operational areas within PTVI with due regard to the company by-laws and prevailing laws and regulations. The use of this Policy may require interpretation, judgment, as well as common sense and communication. Where feasible, the risk management principles adopted by the PTVI Group shall be applied consistently. The scope of this Policy encompasses the following:

a. Principles
b. Risk Management Process
c. Risk Concept
d. Risk Strategy
e. Risk Management Governance Structure

3. References

a. PTVI Code of Conduct
b. PTVI-POL-0005 Human Rights Policy

c. PTVI-POL-0012 Climate Change Policy
d. PTVI-POL-0016 Anti-Corruption Policy
e. PTVI-POL-0019 Sustainability Policy
f. PTVI-POL-0025 Sanctions Compliance Policy
g. PTVI-POL-0032 Water and Water Resources Policy
h. PTVI-POL-0036 Diversity and Inclusion Policy
i. PTVI-POL-0037 Policy for Dam Safety and Geotechnical Mining Structures
j. PTVI-POL-0040 Mining and Metallurgical Waste Management Policy

4. Glossary

a.	Audit Committee:	the committee that assists and provides an objective, non-executive review of the effectiveness of the Enterprise Risk Management (ERM) framework.
b.	BOC:	Board of Commissioners
c.	BOD:	Board of Directors
d.	Emerging Risk:	new or evolving risks with uncertain characteristics, limited data, and potential to significantly affect the Company's strategic objectives, operations, or reputation, arising from shifts in technology, regulation, markets, environment, or stakeholder expectations.
e.	Enterprise Risk Management:	The department that develops and assists the implementation of management policies, methodologies, and tools, promoting integrated communication and disseminating the company's risk management culture.
f.	Integrated Risk Map:	a non-exhaustive tool that contains the set of potential risks proposed by the BOD and approved by the BOC.
g.	Probability Table:	Reference tool used to assess the likelihood or frequency of a risk event occurring.
h.	Risk:	effect of uncertainty on organizational objectives, which manifest itself in many ways and with a potential impact on all dimensions of the business

i. Risk Matrix: contains the risk classification based on a combination of two factors, likelihood and consequence of events. This combined analysis establishes a risk priority scale, with each event being classified as Very High, High, Medium, or Low, which allows comparisons among potential risk events, allowing prioritization for risk treatment.

j. Risk Mitigation Committee: the committee that oversees the implementation and operation of risk management framework and monitors the risk culture and provides advice and recommendation related to risk management including risk appetite references to the BOC.

k. Risk Themes: part of Integrated Risk Map that shows risk categories, including but not limited to People, Sustainability, Institutional Relations and Reputation, Strategic, Cyber, Financial, Planning and Operational Continuity, Geotechnics, and Compliance.

l. Severity Table: Structured reference used to evaluate the potential impact or consequences of a risk event on the organization

5. Principles

The Risk Management should:

- Support PTVI strategic planning, budget, and business sustainability.
- Embed as an integral component of PTVI's management practices, organizational systems, and good corporate governance. This integration is intended to enhance the quality of outcomes and strengthen the accountability of PTVI's decision-making processes.
- Established risk management framework to support the integration of risk management across all functions and activities within the Company. The framework encompasses the following components: integration, design, implementation, evaluation, and continuous improvement throughout PTVI's business processes.
- Implement risk management based on the applicable standards, appropriate organizational structure, and mandate to avoid conflict of interest.
- Implement systematic, measurable, and sustainable risk management to support good corporate governance within PTVI.
- Strengthen the capital structure and asset management of PTVI, by including concepts and assumptions of management based on the risks from operation, maintenance, and asset and logistics.

- Measure and monitor potential risks within PTVI based on a structured methodology used to identify and treat risks arising from its whole business activity, considering the effect of diversification.
- Establish a specialised structure for specific and independent performance, as 2nd Line of Defence, in the assessment of potential operational risks.
- Assess the impact of new corporate actions on PTVI's risk map and risk tolerance.
- Evaluate the implementation of risk management periodically to ensure the effectiveness and sustainability of the company.
- Complying to all prevailing laws and regulations, as well as ensuring that all its operations conform to the standards and requirements delineated in licenses, permits, approvals, and any other form of documentation held by PTVI issued by the authorised government authority. This obligation covers, however not limited to, all statutory provisions, governmental regulations, and industry standards that are applicable, including certifications and implement procedures in accordance with prevailing laws and regulations.

6. Risk Management Process

a. PTVI adopts a structured Risk Management process comprising, at a minimum, the following key activities:
   i. Communication and consultation
   ii. Establishment of risk strategy
   iii. Risk assessment
   iv. Risk treatment
   v. Monitoring and evaluation
   vi. Risk management reporting

b. The implementation of this process is guided by applicable laws, regulations, and the Company's prevailing Risk Strategy, ensuring alignment with both internal governance and external compliance requirements.

7. Risk Concept

- Risk is the effect of uncertainty on the organizational objectives, that manifests in many ways with potential impact on all business dimensions.
- Emerging risks are new or evolving risks with uncertain characteristics, limited data, and potential to significantly affect the Company's strategic objectives, operations, or reputation, arising from shifts in technology, regulation, markets, environment, or stakeholder expectations.
- The Company shall proactively identify, assess, and monitor emerging risks through a scanning process that considers technological, environmental, regulatory, market, and geopolitical developments relevant to the Company. Emerging risks shall be regularly reviewed by the Risk Management function and relevant business units to evaluate their potential impact on strategic

objectives, operations and reputation.

- PTVI classifies risks into several distinct categories, which include operational, project & exploration, cyber, people, sustainability, finance and compliance. Risks must be properly registered in the risk management system by the 1st Line of Defence according to its categories.
- Operational risks are those related to PTVI's operational activities which include:
  i. Health and safety incidents
  ii. Asset integrity and performance
  iii. Property damage and operational interruption
  iv. Quality, availability and logistics of critical supplies
  v. Dam structures
  vi. Geotechnical condition
  vii. Release to environment
  viii. Other risks associated with day-to-day operational activities and Company's operational performance
- Project and exploration risk are relevant potential risks to:
  i. Project management
  ii. Availability, complexity and quality reserves
  iii. Other risks that may affect Company's project and exploration performance
- IT & Cybersecurity risk refers to potential for losses or disruptions resulting from the failure, inadequacy, or misuse of information technology systems, infrastructure, or processes, which may include but not limited to:
  i. IT asset integrity and performance
  ii. Cybersecurity
  iii. Other risks that may affect Company's IT and cybersecurity performance
- People risk refers to the potential for adverse impacts on an organization's performance, reputation, or continuity due to issues related to its human capital and workforce. Such risk include:
  i. Culture, availability and management of talent.
  ii. Outsourcing and partnership.
  iii. Union relations.
  iv. Other risks related to human capital and workforce management.
- Sustainability risk refers to the potential negative impact on an organization's ability to operate responsibly and sustainably over the long term, which include:
  i. Climate change and low carbon agenda
  ii. Water and energy availability
  iii. Biodiversity

iv. Abusive and discriminatory practice
v. Community and indigenous relations
vi. Mine closure
vii. Other risks that may affect Company's environmental, social and governance performance

- Strategy risk refers to potential losses arising from the Company's strategic action such as investment decision, innovation initiatives and geopolitical environment
  i. Portfolio Management
  ii. Innovation and change management
  iii. Geopolitical environment
  iv. Other risks that may affect Company's strategic objectives.
- Market, Macroeconomic & Finance risk refers to potential for losses arising from the Company's financial activities and possibility of adverse impacts resulting from changes in market or macroeconomic conditions. Such risk includes:
  i. Liquidity
  ii. Macroeconomic conditions
  iii. Unit cost & commodity price
  iv. Payment terms
  v. Counterparty credit
  vi. Other risks that may affect Company's financial performance.
- Legal, Compliance & Reputation risk refers to the potential for legal or regulatory sanctions, financial loss, or reputational damage, which includes:
  i. Regulatory compliance
  ii. Legal dispute
  iii. Fraud and Criminal Activities
  iv. Reputation
  v. Other risks that may arise from a failure to comply with applicable laws, regulations, internal policies, or contractual obligations.

BOD proposes the risk categories and themes that compiled as Integrated Risk Map, when necessary, to the BOC for approval, which may take into account the risks posed to the PTVI that may affect Company's business objectives and strategy to maintain its business operation.

8. Risk Strategy

a. The Risk Strategy serves as a reference for the implementation of Risk Management in the Company.

b. The Risk Strategy is developed by the Company's Enterprise Risk Management function and shall

take into consideration the following:

i. Shareholder's risk appetite statements
ii. Company's core competencies
iii. Industry outlook and the Company's positioning within the industry
iv. Company's current business condition
v. The time horizon for achieving corporate targets as outlined in the Long-Term Business Plan or Annual Work Plan and Budget

c. Risk Strategy shall include the following:
   i. Risk Appetite Statement
   ii. Risk Threshold values encompassing Risk Capacity, Risk Tolerance, Risk Appetite, and Risk Limits
   iii. Risk Matrix

d. Risk Appetite Statement is a statement that defines the organization's willingness and ability to take risks in pursuit of its strategic objectives.

e. Risk Threshold is the predefined boundary within which risk levels must remain to ensure alignment with strategic objectives, regulatory requirements, and operational sustainability. It further guides risk-taking decisions, triggers escalation processes, to supports proactive risk mitigation. Risk Threshold values encompassing the following:
   i. Risk Capacity, the maximum amount that the company can bear based on capital, net working capital, liquidity, total company funding capacity, or other agreed threshold values.
   ii. Risk Tolerance, the risk amount that can be tolerated from the Risk Appetite value that is willing to be taken. This value is higher than the Risk Appetite value.
   iii. Risk Appetite, the risk amount that Company is willing to take in achieving expected results.
   iv. Risk Limit, the limit amount that will be distributed and serve as a reference for risk-owning units.

f. The Risk Matrix establishes strategy and governance to be followed in responses to risks, based on the event classification in the Risk Matrix. The Risk Matrix contains the risk classification based on a combination of two factors, probability and severity of risk events. This combined analysis establishes a risk priority scale, with each event being classified as Very High, High, Medium, or Low, which allows comparisons among potential risk events, allowing prioritization for risk treatment. The Severity and Probability Table are tools that help to assess risk events in perspective and prioritise their mitigation activities. The Severity Table is used to assess the progressive severity of impacts in different dimensions. The Probability Table statistically estimates probability of risk occurrence.

g. Risk Strategy is proposed by the BOD and approved by the BOC. Risk Strategy should be periodically reviewed by the Enterprise Risk Management (ERM) function, at least once a year or whenever it no longer reflects the actual or current Company conditions, taking into account the

following considerations:

i. Company's historical performance and achievements.
ii. Company's development and growth plans.
iii. Value and impact of risks that have materialized.
iv. Directives or provisions issued by Shareholders and/or Regulatory Authorities.
v. Other relevant and material factors.

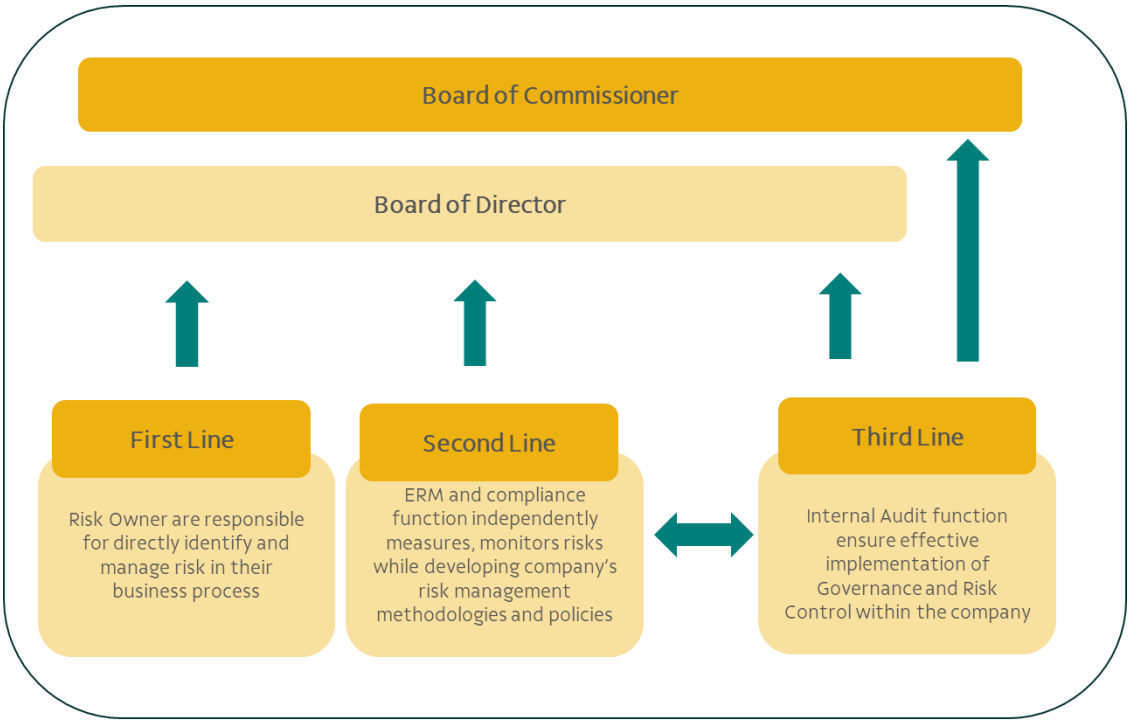
Any changes to the Risk Strategy must be proposed by the BOD and approved by the BOC.

h. The BOD should provide, through human, financial and other resources, by approvals under their authority limits, the necessary supports to the 1st and 2nd Lines of Defences to reduce or eliminate risks to align with Risk Strategy and to evaluate that the risks at continuous monitoring level have effectiveness of controls and timeliness of action plans 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 stoppage of an activity.

9. Risk Management Governance Structure

PTVI applies integrated risk management governance model, based on the concept of three lines defence, optimizing the decision-making communication flow, and reinforcing the alignment among strategy, performance and risk management. To support implementation of risk management in PTVI, the Company is supported by the following risk management bodies:



BOC is responsible to supervise BOD on the management of PTVI to achieve business objectives and purposes. In performing its responsibilities, the BOC is assisted by, (i) the Audit Committee, and (ii) the Risk Mitigation Committee.

BOD is responsible for management and shall at all times act in good faith for the interest of the company. [In carrying out its duties and responsibilities, BOD should manage the risks faced by the Company and optimise any opportunities by ensuring that appropriate systems for risk management are in place and comply with the laws and regulations as well as the relevant standard. The BOD is also responsible in leading the Company toward risk culture that fit with its vision, mission, and values.

1st Line of Defence:

- The 1st Line of Defence, as the risk owner unit, is responsible for identifying and managing risk business processes. It comprises the executors of PTVI's operational and business processes, who register identified risks, assess and develop risk treatment in the entire operating model, implement risk management controls and create respective action plans.
- The 1st Line of Defence is directly accountable for maintaining risks within the tolerable limits defined at the Company and accountable for the execution of the preventive and mitigative controls. It is also accountable for ensuring the integrity and reliability of assets and must halt operations when critical deviations or control failures elevate risks to unacceptable levels.

- The 1st Line of Defence shall monitor compliance with regulations and internal standards, ensuring the effectiveness of controls and timely execution of action plans, and seeking support from relevant governance bodies when necessary. In cases of heightened risk, the 1st Line of Defence are empowered to take immediate preventive or mitigative actions and, if required, escalate for ratification.
- 1st Line of Defence shall manage preventive and mitigative controls, ensure their accuracy, timeliness, and compliance with applicable laws, internal policies, and standards. It must promptly address any identified deficiencies. It also requires performing or reviewing control tests according to defined frequencies, document evidence for critical controls in the Risk Management System for verification purposes and reporting to 2nd Line of Defence if deficiencies are found, especially in critical controls.
- 1st Line of Defence must develop and associate action plans for ineffective or pending controls, monitor their execution and related investments, and formally certify any control and its changes within the Risk Management System.
- The 1st Line of Defence is expected to proactively implement mitigation strategies, manage risks in alignment with PTVI's Risk Management process, continuously assess and monitor the risks, ensure that the action plans established to prevent or mitigate risks, whatever their classification, are being implemented within the deadline, prioritizing actions that lead to reduction of risk level.
- The 1st Line of Defence shall share and provide technical and methodological support regarding the standards and guidelines for risk management established in PTVI operations with related business partners.
- The 1st Line of Defence shall establish Crisis Management and Business Continuity protocols for high-severity risks, comply with technical guidelines from the 2nd Line of Defence, and monitor risk indicators to support continuous improvement. The 1st Line of Defence shall evaluate corrective actions, secure necessary resources, and formally certify risks and associated changes in the Risk Management System.
- Every risk identified by the 1st Line of Defence must be attributed to a risk owner, with a minimum position of manager.

2nd Line of Defence:

2nd Line of Defence consists of Enterprise Risk Management unit and 2nd Line Specialist, to support 1st Line of Defence.

i. Role and responsibilities of Enterprise Risk Management (ERM) unit is as follow:
   - Develop and implement policies, methodologies, processes, and infrastructure, along with an integrated communication system, ensuring standardized Enterprise Risk Management practices at PTVI.
   - Support the 1st Line by providing training and methodological tools and risk infrastructure for the Risk Management process.

- Facilitate knowledge exchange and promote risk prevention culture, ensuring risk awareness across the organization.
- Monitor compliance with the risk management governance structure and ensuring adherence to policies and regulatory requirements.
- Support external disclosure of official Enterprise Risk Management information.
- Report to the Risk Mitigation Committee regarding the Integrated Risk Map, including the status of controls and risk action plans.
- Consolidate decisions from the Risk Mitigation Committee for submission to the Board of Directors, ensuring follow-up on recommendations and assessing the technical effectiveness of controls when applicable.
- Conduct Risk Review for corporate strategic decision, Request for Approval (RFA), and Risk Based Budgeting for annual and capex budget as further governed in the relevant risk management procedures and standard operating procedures (SOPs).
- Conducting periodic or as-needed reviews to ensure the adequacy of risk management policies, strategies, and guidelines, the accuracy of risk assessment methodologies, and the adequacy of the Risk Management Information System.
- Developing strategies for risk management implementation.
- Formulating, evaluating, and submitting proposals for the establishment of Risk Threshold (Risk Capacity, Risk Appetite, Risk Tolerance, and Risk Limits) to the BOD.
- Conducting management of periodic or ad-hoc stress testing to assess the impact of economic condition changes on portfolios or overall performance.
- Managing evaluation process for model accuracy and validating data used for risk measurement.
- Preparing and reporting risk management updates such as consolidation of Risk Profile to the BOC, BOD and RMC.
- Serves as the framework owner and provides oversight to ensure enterprise-level consistency and integration by validating that risk registers, particularly those in high-risk areas or top risks, align with taxonomy, appetite, and strategic risk themes.

ii. Role and responsibilities of 2nd Line Specialist is as follows:

- Act within corporate guidelines for risk management.
- Define methodologies, technical, technological, and management standards, as well as risk and asset reliability indicators to be adopted by the 1st Line of Defence.
- Establish methodologies and technical condition criteria for critical control elements.
- Conduct independent evaluations of overlooked controls, assessing effectiveness related to potential risks as a compensatory measure for the 1st Line of Defence. If deviations are found in existing controls for Very High and High criticality risks, they have the authority to define immediate actions to be executed by the 1st Line of Defence, including stopping asset operations if necessary.
- Support the 1st Line of Defence by verifying whether risks have adequate mapped controls

and whether implemented barriers are the most effective for mitigating specific risks.

- Assess the implementation of standards and indicators across operational, commercial, project, support, and administrative areas, ensuring independence and transparency.
- Escalate relevant potential risks to the BOD if preventive action decisions require additional support.
- Provide input on Top Risks, Risk Strategy, and Key Risk Indicators (KRIs) to ensure alignment with business objectives and evolving risk landscapes.
- Support the Enterprise Risk Management (ERM) as Subject Matter Experts (SMEs) in risk reviews, providing technical insights and validation of risk assessments.
- Provide data support along with technical support and standardized guidance regarding risk management.
- Verify the controls and action plans, according to the defined planning.
- Disseminate knowledge and foster good practices, ensuring standardized treatment for similar risks.
- Ensure that the appropriate recommendations from the insurers are considered in risk management process.
- Serves as the primary verifier of risk register entries by reviewing submissions from the 1st Line of Defence to ensure risk descriptions are complete, causes and impacts are clearly stated, ratings align with criteria, and controls, indicators, and treatment plans are properly linked, while also providing feedback to enhance accuracy and consistency while other 2nd Line Specialists (e.g., Growth Project Risk, Compliance) may provide input or guidance to ensure consistency within their respective domains.

3rd Line of Defence:

- The 3rd Line of Defence is composed of areas that is independent from PTVI's administration, which include the Internal Audit that 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.
- Ensuring governance control and risk control are effectively implemented by PTVI.
- Monitoring and evaluation of the effectiveness of PTVI's key risk management process, as defined by the BOC.
- Evaluating the effectiveness and efficiency of processes, as well as compliance with guidelines related to engineering, maintenance, geotechnics, and Health and Safety area, by engaging specialised technical consultant when required.
- Monitoring and evaluation of governance, compliance, and internal controls processes, including the effectiveness of the activities of the 1st and 2nd Lines of Defence.
- Consulting and 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

the responsibility inherent to the duties of the risk owners and the 2nd Line of Defence.

- Communicating to the responsible management and competent governance bodies about exposure to significant risks and control deficiencies.

10. Risk Management Maturity Assessment

a. The effectiveness and quality of Risk Management implementation are evaluated by using applied key indicator for risk management maturity Level. The technical guidelines, assessment dimensions, and evaluation criteria for determining the maturity level of Risk Management are based on applicable laws, regulations, and internal policies.

b. The assessment of Risk Management maturity shall be conducted periodically, either through self-assessment or by engaging an independent assessor, to ensure objectivity and alignment with applicable standards and governance requirements.

11. Consequence Management

Non-compliance with this Policy is subject to the provisions set forth in PT Vale's Consequence Management Policy.

12. Language

This Policy is made in English and Bahasa Indonesia. In the event of any inconsistency between English and Bahasa Indonesia (including on the meaning or interpretation of certain provision/wording), the English version shall prevail, and the Bahasa Indonesia version will be deemed to be amended to conform with and to make the Bahasa Indonesia version consistent with the English version.

13. Final Provisions

Other matters that are not yet or not sufficiently regulated in this Policy shall be regulated subsequently.