INTERNAL POLICY

RISK MANAGEMENT POLICY

Adopted by Audit Committee of Jaguar Mining

March 2020

Table of contents

Approval and revision history

Aproved by		
Version	**Name / title**	**Date**
0	Audit Committee	23/03/2020

Risk Management Policy

1. PURPOSE

The purpose of this policy is to provide guidance of Jaguar's Risk Management since identifying, evaluating, treating, reporting and monitoring Jaguar's risks. Also, guide risk management methodology, in addition to strengthening a risk management culture.

2. APPLICABILITY / SCOPE

This policy applies to all company and its guidelines must be observed and serve as a source of permanent consultation to implement and / or define risk and opportunity management strategies.

3. POLICY REQUIREMENTS

This policy complements Jaguar's Code of Ethics and Conduct, other policies and provides guidelines for risk management. This policy doesn't intend to replace any applicable laws.

The terminology of this document and the methodologies to be applied during the risk assessment are aligned with the COSO Enterprise Risk Management - ERM structure and ISO 31000.

4. ROLES AND RESPONSIBILITIES

Board of Directors

Responsible for this policy and appointed the Audit, Risks and Compliance manager to oversee the administrations of this policy and report directly to Audit and Risk Committee.

Audit and Risk Committee

Evaluate and monitor Jaguar's risk exposure, deliberating on recommendations prepared by Managers and Audit, Risks and Compliance area and subsidizing resources for implementation of effective internal controls and risk mitigation strategies.

Managers

Ensure the implementation of action plans for risk mitigation, be proactive in identify risks, always communicating them to Audit, Risks and Compliance area.

Compliance Area

Ensure the implementation of the methodology defined for the management and mitigation of risks identified at Jaguar;

Identify, evaluate, communicate and monitor actions to mitigate Strategic and Operational Risks;

Report to the Audit Committee the results of the Strategic and Operational Risk assessments.

I. Roles and attributions of the governance model in the three lines of defense

Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

The three lines of defense model brings several corporate functions and teams, including governance structures and agents, allowing control of identified risks.

First line of defense: carried out by managers and those directly responsible for the processes: it includes the functions they manage and have responsibility for the risks;

Second line of defense: carried out by corporate risk management, compliance or other control practices, for example, and which includes the functions that monitor the integrated view of risks;

Third line of defense: performed by internal audit: provides independent assessments through the monitoring of internal controls.

5. DEFINITIONS

Impact: the extent to which the risk, if realized, would impact the organization. Factors that may help define the impact rating may include financial effect, damage to assets, reputation impacts, ability to achieve key objectives, etc.

Inherent risk: the classification of probability and impact for a given risk from an industry perspective, without considering the specific processes, activities or controls of the company that were designed and implemented to specifically manage or mitigate the risk.

Management and control activities: Activities established by management to mitigate risk and may include specific monitoring activities, policies, procedures, information technology controls, physical restrictions, authorizations and other activities. It is the extent to which management and control activities are effectively designed, operated, and aligned to risks that mitigates either the impact or likelihood of an inherent risk occurring.

Likelihood: the likelihood of a risk occurring over a predefined period. In most cases, this is defined in one year, but it can be adjusted to be in line with the company's planning. In some cases, the frequency of the occurrence can also be considered.

Risk: A risk is any event or circumstance that could affect the achievement of business objectives. Risk is defined in terms of the likelihood of occurrence, and impact in the event that it occurs.

Risk appetite: Risk appetite is the exposure that the company is willing to accept in order to achieve its goals and objectives, preserve and create value, being directly related to its strategy.

Risk management and control activities: Risk Management and Control Activities include initiatives, policies, processes and procedures, physical restrictions, guidelines, rules, etc. There are two types of activities: a) preventive - whose purpose it is to prevent, reduce or mitigate risks within the business, area, project, etc., b) detective - whose purpose it is to identify and trigger a desired response to risks once they have occurred within the business, area, project, etc.

Risk matrix: Tool that indicates, graphically, what are the risks considering the likelihood and impact vectors.

Risk register: Document used as a repository of all identified risks, which may include additional information for each risk.

Residual risk: the likelihood and impact rating for a risk determined after the consideration of the Company's specific processes, activities or controls that have been designed and implemented to specifically manage or mitigate the risk.

6. GUIDELINES

The guidelines of this policy define and characterize Jaguar's Risk Management process. In order to have good risk management and control, it is essential that risks are quantified and qualified. By doing this, it is possible to eliminate or reduce possible financial losses.

The risks are classified into four distinct groups below:

- **Strategic**: events that are related to senior management decision-making and can generate substantial loss in the organization's economic value.

- **Operational**: events that may compromise the company's activities, usually associated with failures, deficiencies or inadequacies of internal processes, people and systems, or external events;
- **Financial**: events that may compromise the company's ability to count on the budget and financial resources necessary to carry out its activities, or events that may compromise its own budget execution;
- **Compliance**: events related to corruption, fraud, irregularities, legal and / or ethical and conduct deviations that may compromise the values and standards established by Jaguar and the achievement of its objectives.

6.1. Risk Identification

The risks that can affect the company's goals are identified through rounds of discussions with the Board, Managers and designated persons, in addition to benchmarking on related materials.

6.2. Risk Assessment

The identified risks are consolidated and subsequently evaluated according to the impact and likelihood (classified in the "Risk Assessment Criteria" approved by the board), in addition to degree of maturity of controls (tested by internal audit).

6.3. Risk Matrix

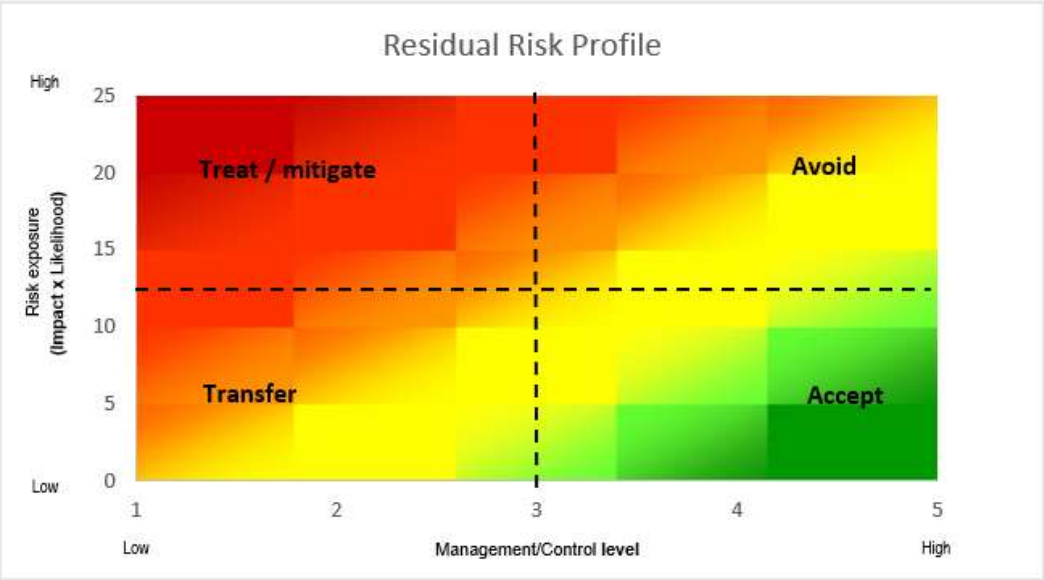
The Risk Matrix is used during the risk assessment to define various levels of risk as a product of the categories of likelihood and impact of damage. The Matrix increases the visibility of risks and assists in making management decisions.

Impact						
	5	Medium	Medium	High	High	High
	4	Medium	Medium	Medium	High	High
	3	Low	Medium	Medium	Medium	High
	2	Low	Low	Medium	Medium	Medium
	1	Low	Low	Low	Low	Medium
		1	2	3	4	5
		Likelihood				

6.4. Risk treatment

- **Avoid:** It aims to eliminate the root cause of the risk, implementing actions to bring the risk probability to zero.

- **Treat / mitigate:** Seeks to reduce the probability of occurrence or the impact of a risk to a level below the acceptable limit.
- **Transfer / share:** Activities that aim to reduce the impact and / or the likelihood of risk occurring through transfer or, in some cases, sharing part of the risk (gives the other party responsibility for its management).
- **Accept:** In cases where the probability of occurrence and impact are low or nothing can be done, the company can simply accept the risks.



6.5. Risk Communication

The areas update the status of the actions for monitoring the risks identified through the “Risk Management Report” - Annex I.

Risk mitigation actions are reported quarterly to the Audit Committee by the Audit, Risk and Compliance area.

7. MAINTENANCE OF RECORDS

The company must maintain appropriate internal controls and records in place. The Risk Register must be duly filed by the Risks area.

8. COMMUNICATION OF THE POLICY

All employees involved in the risk identification and assessment process shall be informed of this Policy.

9. MONITORING AND REVIEW

Internal Audit manager will monitor the effectiveness and review the implementation of this policy, regularly considering its compliance, suitability and effectiveness. Any improvement identified will be made as soon as possible.

10. EXCEPTIONS AND VIOLATIONS

Exceptions to this policy are not acceptable.

11. MAINTENANCE AND REVIEW

The Compliance Policy should be reviewed in its entirety at least every two years.