RISK MANAGEMENT POLICY

THE ORISSA MINERALS DEVELOPMENT COMPANY LIMITED

(A Govt. of india Enterprise)

Contents

Risk Management Policy

1.1 Objectives of the Policy

The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the policy establishes a structured and disciplined approach to Risk Management, including the development of the Risk Matrix, in order to guide decisions on risk related issues. The specific objectives of the Risk Management Policy are:

1. To ensure that all the current and future material risk exposures of the company are identified, assessed, quantified, appropriately mitigated and managed.

2. To establish a framework for the company's risk management process and to ensure companywide implementation.

3. To ensure systematic and uniform assessment of risks related with projects and operational mines.

4. To enable compliance with appropriate regulations, wherever applicable, through the adoption of best practices.

5. To assure business growth with financial stability.

1.2 Risk Management Policy

In order to fulfill the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:

1.2.1 Principles of Risk Management

1. All business decisions will be made with the prior information and acceptance of risk involved.
2. The Risk Management Policy shall provide for the enhancement and protection of business value from uncertainties and consequent losses.
3. All employees of the company shall be made aware of risks in their respective domains and their mitigation measures.
4. The risk mitigation measures adopted by the company shall be effective in the long-term and to the extent possible be embedded in the business processes of the company.
5. Risk tolerance levels will be regularly reviewed and decided upon depending on the change in company's strategy.
6. The occurrence, progress and status of all risks will be promptly reported and appropriate actions be taken thereof.

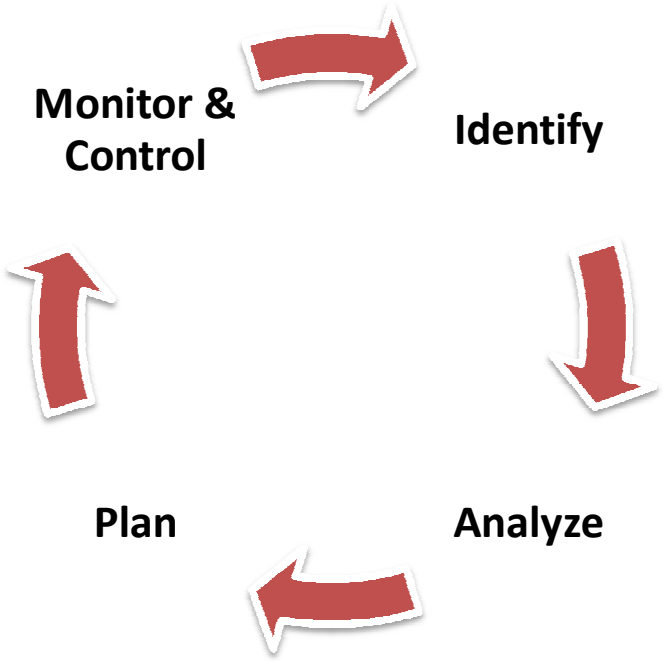
1.2.2 Risk Management Policy Statement

The policy statement is as given below:

1. To ensure protection of shareholder value through the establishment of an integrated Risk Management Framework for identifying, assessing, mitigating, monitoring, evaluating and reporting of all risks.
2. To provide clear and strong basis for informed decision making at all levels of the organization.
3. To continually strive towards strengthening the Risk Management System through continuous learning and Improvement.

1.3 The Steps in Managing Risk

In order to fulfill the objectives of this policy and lay a strong foundation for the development of an integrated risk management framework, the policy outlines the following guiding principles of Risk Management:



The process of Risk Management involves the following:

1. **Risk Identification & Categorization** - During risk identification, the sources of risk, potential risk events, and symptoms of risk are identified and classified as Strategic Risk / Business Risk / Operational Risk.

2. **Risk Analysis** - During risk analysis, the value of opportunities to pursue vs. the threats to avoid, and the opportunities to ignore vs. the threats to accept are assessed.

3. **Response Planning** - During response planning, risk management and contingency plans are developed.

4. **Risk Monitoring & Control** - During risk monitoring and control, corrective action plans are developed, implemented, and monitored.

1.3.1 Risk Identification and Categorization

During risk identification potential sources of risk and potential risk events are identified.

As defined earlier, risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives.

Key Characteristics by which risks can be identified are:

- Risks are adverse consequences of events or changed conditions
- Their occurrence may be identified by the happening of triggering events
- Their occurrence is uncertain and may have different extents of likelihood

Recognizing the kind of risks that company is/may be exposed to, risks will be classified broadly into the following categories:

Strategic Risk: includes the range of external events and trends (like Government policy, competition, court rulings or a change in stakeholder requirements) that can adversely impact the company's strategic growth trajectory and destroy shareholder value.

Business Risk: includes the risks associated specifically with the company and having an adverse impact on the company's capability to execute activities critical for business growth, thereby affecting its near-term performance. E.g. occurrence of a risk event delaying the mining activity leading to the deferment of revenues expected or expiry of mining lease leading to closure of mining activities and related operations thereof.

Operational Risk: are those risks which are associated with operational uncertainties like unpredictable changes in water levels, force majeure events like floods affecting operations, internal risks like attrition etc

Once the risks are identified, all identified risks should be documented in a Risk Register. The following information should be included in the Risk Register for each of the risks identified:

- A brief description of the risk
- Category of Risk
- Risk Trigger
- Potential Outcome
- Raised by
- Date Raised
- Source

The risk trigger is the event that would need to happen in order for the potential outcome to occur. Risk triggers are usually expressed with some sort of dependency, or qualifier. For example, a risk trigger might be that a resource on the project leaves. This might easily be accounted for by utilizing other resources. But if a resource with key skills or knowledge leaves, then the project may be significantly impacted. This approach is suggested in order to clarify the thought process of identifying risks. When the risk trigger occurs, the risk is no longer a risk, but has materialized into a problem/issue that needs resolution.

The various risks that the company is or can be exposed to are identified in the Risk Matrix.

1.3.2 Risk Analysis

After a risk or group of risks has been identified and documented, risk analysis should be performed. During risk analysis, each potential risk event is analyzed for:

- The likelihood that the risk will occur
- The impact of the risk if it occurs

Risk probabilities are defined in Section-1 of the Appendix. Risk impact definitions are defined in Section-2 of the Appendix. Impacts can be assessed against cost, schedule, scope, and/or quality. If the risk event affects more than one dimension and the scores are different, the higher impact definition should be utilized.

Once the appropriate risk impact and likelihood are selected, the risk score can be determined. The risk likelihood and impact matrix is shown in section-3 of the Appendix. The matrix shows the combination of impact and likelihood that in turn yield a risk priority (shown by the red, yellow, and green colored shadings).

Risk priority is utilized during response planning and risk monitoring/control. It is critical to understand the priority for each risk as it allows the project team to properly understand the relative importance of each risk.

Risk impact analysis can be qualitative or quantitative.

Qualitative Analysis

Qualitative analysis is a quicker and usually more cost-effective way to analysis risks (as opposed to quantitative analysis). Analysis should be performed with the goal of gathering data on:

- The likelihood of the risk occurring (using definitions from Section-1)
- The qualitative impact on the project (using definitions from Section-2)
- The quality of the risk data being utilized (e.g. how reliable is the data?)

Quantitative Analysis

Quantitative analysis utilizes techniques such as simulation and decision tree analysis to provide data on:

- The impact to cost or schedule for risks
- The likelihood of meeting project cost and/or schedule targets
- Realistic project targets on cost, schedule, and/or scope

Qualitative analysis should occur prior to conducting quantitative analysis. Not every risk needs to go through quantitative analysis. If quantitative analysis is to be used, then this section should contain information on:

- Defined criteria for which risks go through quantitative analysis
- Technique(s) to be utilized

- Expected outputs of quantitative analysis

The results of risk analysis should be documented in the risk register. The following information shall be entered in the register:

- Risk impact
- Risk likelihood
- Risk matrix score – computed by the risk register spreadsheet after impact and likelihood are entered
- Risk priority – computed by the risk register spreadsheet after impact and likelihood are entered
- Qualitative impact – descriptive comments about the potential risk impact

1.3.3 Response Planning

During response planning, strategies and plans are developed to minimize the effects of the risk to a point where the risk can be controlled and managed. Higher priority risks should receive more attention during response planning than lower priority risks. Every risk threat should be assigned an owner during response planning.

Risk Strategies

There are several methods for responding to risks:

1. Avoid

Risk avoidance involves changing aspects of the overall project management plan to eliminate the threat or relaxing the objectives that are in threatened (e.g. extending the schedule or reducing the scope). Risks that are identified early in the project can be avoided by clarifying requirements, obtaining more information, improving communications, or obtaining expertise.

2. Transfer

Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat, it simply makes another party responsible for managing it.

3. Mitigate

Risk mitigation involves reducing the likelihood and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans are examples of risk mitigation.

4. Accept

Acceptance is often taken as a risk strategy since it is very difficult to plan responses for every identified risk. Risk acceptance should normally only be taken for low-priority risks. Risk acceptance can be passive, where no action is taken at all, or active. The most common active approach to risk acceptance is to develop a cost and/or schedule reserve to accommodate known (or unknown) threats.

The results of response planning should be documented in the risk register. The following information shall be entered in the register:

- Response strategy (avoid, transfer, mitigate, or accept)
- Response notes (description of plan) – if a mitigation approach is taken, specific trigger points that require aspects of the contingency plan to be executed should be documented
- Risk owner

1.3.4 Risk Monitoring and Control

Planned risk responses should be executed as required, but the mining and other activities should also be continuously monitored for new and changing risks. During risk monitoring and control the following tasks are performed:

- Identify, analyze, and plan for new risks
- Keep track of identified risks and monitor trigger conditions
- Review performance information (such as progress/status reports, issues, and corrective actions)
- Re-analyze existing risks to see if the likelihood, impact, or proper response plan has changed
- Review the execution of risk responses and analyze their effectiveness
- Ensure proper risk management policies and procedures are being utilized

The results of risk monitoring and control should be documented in the risk register. The following information shall be entered in the register:

- Status – valid statuses are:
  - ✓ Identified – Risk documented, but analysis not performed
  - ✓ Analysis Complete – Risk analysis done, but response planning not performed
  - ✓ Planning Complete – Response planning complete
  - ✓ Triggered – Risk trigger has occurred and threat has been realized
  - ✓ Resolved – Realized risk has been contained
  - ✓ Retired – Identified risk no longer requires active monitoring (e.g. risk trigger has passed)
- Trigger Date – if the risk has been triggered
- Notes

1.4 Risk Organization Structure

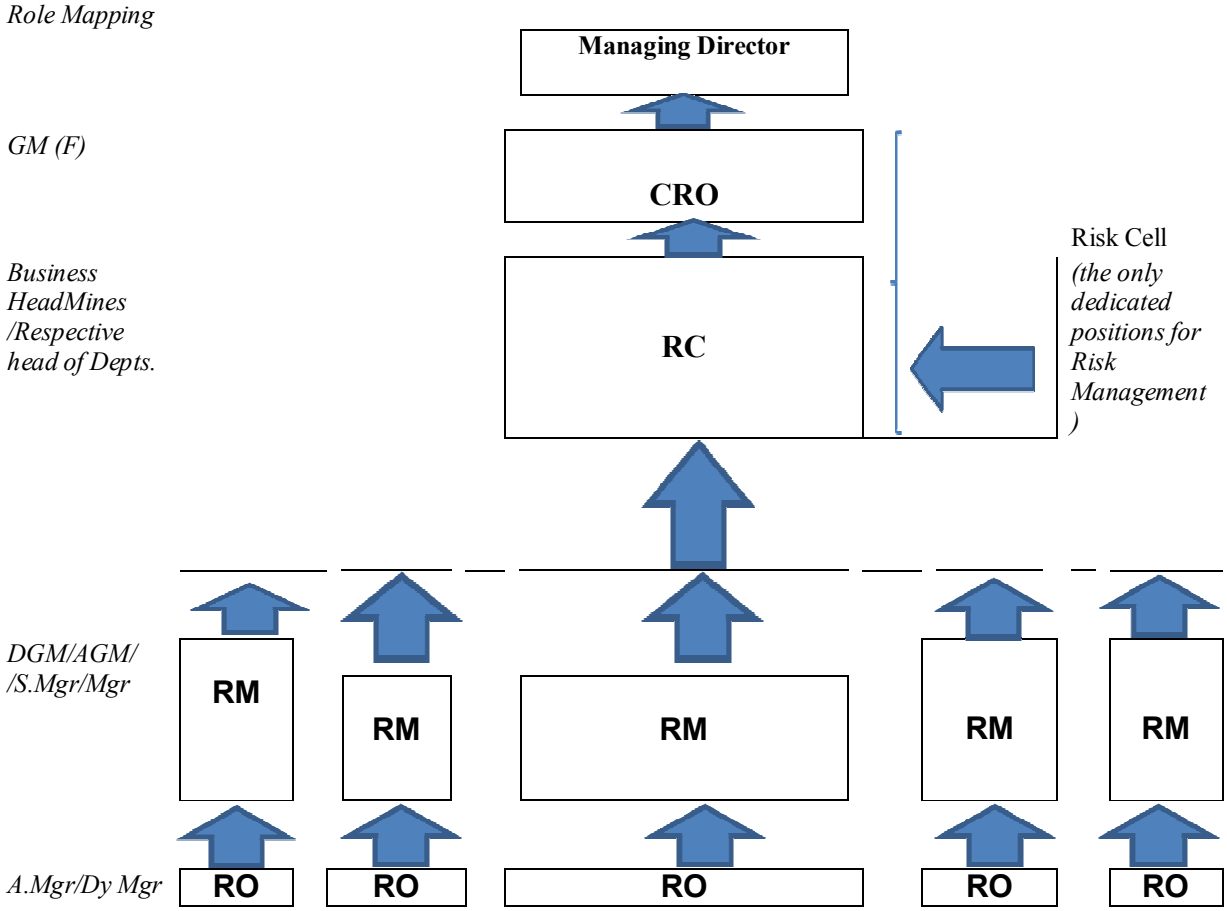
The Risk Management Policy will be implemented through the establishment of a Risk Organization Structure. At the core, a Risk Cell comprising of the Chief Risk Officer (CRO) and the Risk Controller (RC) has to be formed (please refer to figure below). The CRO will have to be of the level of General Manager while the RC will have to be of the rank of Business Head at Mines office/ respective head of departments as authorized by the management from time to time. The Risk Managers (RM) and Risk Officers (RO) will be line functionaries, with cross-functional job descriptions – they will perform individual line duties, and also report to the Risk Cell. The RMs and ROs will therefore hold additional responsibilities for risk reporting beyond their line duties.

The overall monitoring of the Risk Cell will be done by the Managing Director. The Board will review the status and progress of the risks and risk management system on a regular basis through the Audit Committee.

All personnel forming a part of the Risk Organisation Structure have to be trained on the company's risk management system.

Following shall be the Risk Organization Structure for the company

Role Mapping



CRO- Chief Risk Officer,
RC-Risk Controller
RM-Risk Manager,
RO-Risk Officer

1.4.1 Roles and Responsibilities

a) The Board will review the risk management policies and system periodically.

b) The Managing Director will be responsible for ensuring that the risk management system is established, implemented and maintained in accordance with this policy.

c) Assignment of responsibilities in relation to risk management will be the prerogative of the Chief Risk Officer.

d) Risk Controller will be accountable to the Chief Risk Officer. The Risk Managers will report to the Risk Controller for the implementation of this Policy within their respective areas of responsibility.

e) Risk Managers will also be accountable to the Risk Controller for identification, assessment aggregation, reporting and monitoring of the risk related to their respective areas

f) Risk Officers will be responsible for identification, preliminary assessment, reporting and monitoring the risks related to their individual projects.

APPENDIX

1. Risk Likelihood Definitions

The following chart shows risk likelihood definitions. During risk analysis the potential likelihood that a given risk will occur is assessed, and an appropriate risk likelihood is selected from the chart below.

Likelihood Category	Likelihood	Description
Almost Certain	0.90	Risk event expected to occur
Likely	0.70	Risk event more likely than not to occur
Possible	0.50	Risk event may or may not occur
Unlikely	0.30	Risk event less likely than not to occur
Rare	0.10	Risk event not expected to occur

2. Risk Impact Definitions

The following chart shows risk impact definitions across each of the potentially impacted project areas (cost, schedule, scope, and quality). During risk analysis the potential impact of each risk is analyzed, and an appropriate impact level (0.05, 0.10. 0.20, 0.40, or 0.80) is selected from the chart below.

Project Objective	Insignificant 0.05	Minor 0.10	Moderate 0.20	Very High 0.40	Extreme 0.80
Cost	Insignificant cost impact	< 10% cost impact	10-20% cost impact	20-40% cost impact	> 40% cost impact
Schedule	Insignificant schedule impact	< 5% schedule impact	5-10% schedule impact	10-20% schedule impact	> 20% schedule impact
Scope	Barely noticeable	Minor areas impacted	Major areas impacted	Changes unacceptable to sponsor	Product becomes effectively useless
Quality	Barely noticeable	Only very demanding applications impacted	Sponsor must approve quality reduction	Quality reduction unacceptable to sponsor	Product becomes effectively useless

3. Risk Likelihood and Impact Matrix

The risk likelihood and impact matrix shows the combination of risk impact and likelihood, and is utilized to decide the relative priority of risks. Risks that fall into the red-shaded cells (Devastating) of the matrix are the highest priority, and should receive the majority of risk management resources during response planning and risk monitoring/control. Risks that fall into the orange shaded cells (Major) of the matrix are the next highest priority followed by risks that fall into the light orange, yellow and green-shaded cells.

			Impact				
			Extreme	Very High	Moderate	Minor	Insignificant
			Threats				
Likelihood	Almost Certain		Extreme	Extreme	Very High	Moderate	Minor
	Likely		Extreme	Very High	Moderate	Minor	Minor
	Possible		Very High	Moderate	Minor	Minor	Insignificant
	Unlikely		Moderate	Minor	Minor	Insignificant	Insignificant
	Rare		Minor	Minor	Insignificant	Insignificant	Insignificant