maithan alloys ltd
CIN: L27101WB1985PLC039503
Regd. Office: 'Ideal Centre', 4th Floor, 9 AJC Bose Road, Kolkata – 700 017
e-mail: office@maithanalloys.com, website: www.maithanalloys.com
Ph.: 033- 4063-2393; Fax: 033-2290-0383

RISK MANAGEMENT POLICY

(as amended on 16th November, 2018)

Preface

The phrase "NO RISK NO GAIN" is known since the inception of business world. It was left to the Insurance Companies, to cover the risk which was the only way to manage the risk. However, importance of risk management has been growing steadily during the last several years. There is increasing awareness and expectation in India and abroad of the need to manage risks, rather than leaving them solely to insurance.

The risk environment has been evolving rapidly, as advancing technological and social developments bring forth new or hitherto dormant risks associated with such phenomena such as competitions, hazardous materials, pollution, electronic data, and exposure to legal and political liability. The Company has an obligation to be fully aware of the state of the art in risk management and to prevent losses and unnecessary expenditures.

Risk management can be extremely cost-effective when departments assess their risks properly and determine the most economical way to avoid them entirely, or reduce them to a minimum and limit potential expenditures arising from accidents or emergencies.

Risk management is a logical step-by-step process to protect, and consequently minimize risks to the Company's property, interests and employees. Risk includes the chance of damage to or loss of company's property, and the chance of incurring second- or third-party liability to other persons. There are four phases in risk management:

before an incident:

Phase 1 - identifying risks and the departments exposed to and in control of the risks; and
Phase 2 - Minimizing risks and their cost;

during an incident:

Phase 3 - containing the effects of any damaging or harmful incident; and

after an incident:

Phase 4 - compensating or restoring and recovering in the event of such incidents, and providing feedback of information as a basis for improving the management system.

Policy objective

The objective of this policy is to safeguard the company's property, interests and certain interests of employees during the conduct of company operations.

Policy statement

It is Company's policy to identify and reduce or eliminate risks to its property, interests and employees, to minimize and contain the costs and consequences in the event of harmful or damaging incidents arising from those risks, and to provide for adequate and timely compensation, restoration and recovery.

Application

This policy applies to:

- departments and any division or branch of the company, including; and

- every individual appointed or employed as a servant of the company. and former servant of the Company and a deceased servant of the Company. It does not include any person appointed or employed by or any person engaged under a contract for services.

Authority

This policy is issued pursuant to the requirement of Clause 49 of the Listing Agreement.

Policy requirements

Identification

1. Every department must identify the potential perils, factors and types of risk to which their assets, program activities and interests are exposed and report to the Audit committee.

Minimization

2. Departments must analyze and assess the risks identified, and design and implement cost-effective risk prevention, reduction or avoidance control measures.

3. Departments must:

(a) select underwriting options;

(b) self-underwrite the risks to which the Company alone is exposed and over which it generally has control, and provide for and absorb, through their annual appropriations, any cost that may arise from self-underwriting;

(c) ensure that contractors do not procure insurance on risks that are clearly the responsibility of the Company, and that contractors are not indemnified by the Company against the risks to which only the contractors are exposed.

4. Departments must plan and budget for containment, compensation, restoration and disaster recovery.

Containment

5. Departments must activate emergency organizations, systems, and contingency plans, and initiate recovery measures.

Compensation, restoration and recovery

6. Departments must:

(a) investigate incidents to determine their causes;

(b) assess the extent and value of damages and determine potential legal liability; and

(c) make incident reports.

7. Departments must repair or replace damaged assets and operating systems to return operations to normal as soon as possible.

8. Departments must:

(a) report each fiscal year in the annual accounts, all payments of claims against the company; all ex gratia payments; court awards; and all losses of Rs. 10,000 or more including accidental destruction of, damage to, or theft of, assets that would normally be covered by insurance had insurance existed;

(b) report to the appropriate law enforcement agencies losses over Rs. 10,000 which are due to suspected illegal activity; and

(c) maintain their own data-base as part of the feedback system of management information.

9. Departments must establish new or improved measures to prevent the recurrence of incidents, and to recover from disasters.

Monitoring

The Audit Committee will review the effectiveness of this policy in departments to manage the risks to which they are exposed. The impact of the policy on departmental operations and performance will be gauged by how well the department has: identified and minimized its risks; contained the effects of any damaging or harmful incident; and achieved adequate and timely compensation, restoration and recovery.

Feedback on the implementation and the effectiveness of the policy will be obtained from each departmental.

Every Department must submit their report under this policy to Audit Committee.

Enquiries

All enquiries about this policy should be directed to the official designated by each department as responsible for risk management and, when appropriate, to legal services. When required, officials should then refer inquiries to either Managing Director or Joint Managing Director.

Appendix B - Guidelines

Introduction

These guidelines deal with: identifying and minimizing risks to prevent an incident; containing damages or harmful effects in the event of an incident; compensating or restoring and recovering following an incident; and providing feedback to improve the risk management system (see Appendix A).

Phase 1 - Identifying risk

1.1 Identifying operations and assets at risk

In the first phase of risk management all of the operational areas and assets of the department should be identified, for example:

- owned or leased real and personal property, such as machinery, buildings, transport, and inventories;
- contracting for construction, goods and services, and ongoing sources of supply;
- cash, accounts payable and lending;
- internal audit;
- information storage and transfer, such as record keeping, mail distribution, telecommunications, and electronic data;
- Company activity; and
- toxic operations and waste
- injury and illness:
- motor vehicles and other employee-owned transportation, personal property during relocation, and personal property in Crown-owned living accommodation:

Damage to employees' effects within the scope of employment is covered in the Policy on Claims and Ex Gratia Payments. Indemnification and legal assistance.

As described below, potential perils, factors, and types of risks present in each of the foregoing should then be identified for subsequent threat assessment and analysis as an input to the minimization phase. This is to determine the risk exposure as a basis for deciding on the need for, and extent of, further risk management phases. It is also to ensure that the system for dealing with a specific risk is compatible with those of other risks in the same area.

1.2 Perils

Each peril should be identified to establish probable exposure, i.e. the degree of risk and its cost, determine alternatives for minimizing them and develop control procedures. Some of the perils that threaten operations and assets and create risks include fire, collision, theft, fraud, security leaks, violence, climate and earthquakes.

1.3 Factors

Factors influencing risks should be identified. They include: acts of nature; human inefficiency, negligence, error, and willfulness; and physical factors such as the availability and quality of materials and the state of a particular technology. Factor should be identified as either External or Internal Factors. They include.

Internal Factors

- Financial Reporting Risk
- Liquidity and Leverage
- Concentration of revenues
- Compliance with laws and regulations
- Human Resource Management

External Factors

- Macro Economic Factors
- Exchange Rate Fluctuations
- Political Environment
- Competitive Environment
- Inflation and cost structure
- Security and business continuity
- Engagement and business continuity
- Engagement execution
- Culture, values and leadership

1.4 Types of risk

Each risk-bearing activity should be identified as one that is either: strictly internal to the company; or partly or wholly related to the actions or omissions, and property of other parties with which the company comes into contact, on or off company premises.

This distinction has important implications for determining the respective obligations or potential liabilities, the degree of control that can be exercised over the probability of chance occurrences, the effect these occurrences may have on the government, and the selection of the appropriate underwriting option.

Information Risk:
It is the process of identifying information assts, assigning appropriate values, identifying threats to those assets, measuring or assessing risk and then developing strategies to manage it.

Strategic Risk :
Risk arising due to poor marketing strategy/acquisitions strategy, changes in consumer behavior, poor product launches

Financial Risk-
It is risk of financial loss of the Company which includes

- Market risk
- Foreign Exchange Risk
- Interest Risk

- Currency Risk
- Liquidity Risk
- Credit Risk

Operational Risk :
it is risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.

Phase 2 - Minimizing risk

2.1 Minimization

The minimization of risk is the second phase of risk management. It is founded on a thorough analysis of the identified risks in order to assess their potential threat to operations and assets, and to determine the degree of exposure (frequency and severity) as a basis for:

(a) avoiding risk by eliminating or radically reducing the risk by considering alternatives to current or proposed activities. For example, an activity could be cancelled or the risk shared with or transferred to others, or

(b) when acceptance of the risk is inevitable, developing and implementing cost-effective risk control practices such as loss prevention and reduction, including safety training, early detection, security precautions, emergency procedures or design changes; and

(c) minimizing the financial consequences by considering options such as self-underwriting, when the risks are clearly internal to the company, ensuring that contractors have adequate insurance, or transferring the financial exposure to insurers; and

(d) planning and budgeting appropriate measures for potential containment, compensation, restoration and recovery.

As described below, each of the assets or operational areas identified may require analyses of the potential liabilities, underwriting, and financial aspects of risk minimization, together with political, diplomatic, administrative and contracting considerations.

2.2 Analysis of potential liability

"Liability" is defined as being under an obligation; for example, to make good any loss or damage. The determination of potential liability normally requires a legal opinion.

The extent to which the Company or other persons may be liable, singly or jointly, and directly or vicariously, should be determined by examining:

- the potential for creating an employer-employee relationship;
- whether there is an agency relationship with the Company;
- whether the activity is fulfilling a need of the Company, or whether it is a commercial undertaking with clients providing a product or service not needed by the Company;
- whether a Company-operated activity is a commercial type of undertaking and should, more appropriately, conform with commercial practices and obtain liability insurance;

2.2.1 Property liability

Potential liability affecting property should be determined by identifying:

- the ownership of the property and its location, for example, whether it is on the Company's or a contractor's premises;
- normal commercial practices and whether a limitation of liability exists.

2.2.2 Company employees' liability

The potential liability of the Company, because of the actions of its employees or agents, should be determined by identifying:

- the degree to which employees are involved;
- whether legislation and administrative policy protecting or employees applies, and
- the extent to which potential liability of personnel engaged in the activity.

2.3 Underwriting analysis

Underwriting encompasses the various ways that financial protection against the potential consequences of risk can be arranged. To underwrite means to assume the financial consequences of the occurrence of a specific peril.

2.3.1 General

Underwriting options that should be considered, either separately or in combination, include:

(a) self-underwriting, when the Company assumes the responsibility to underwrite specific risks, generally those over which it has control, including the Company's established liabilities. The Company's policy of self-underwriting most of its assets and program activities applies to:

- in-house risks when outsiders entities are not involved; and
- risks of incidents involving third parties to the extent that the company is liable, or that damages or losses cannot be recovered, or that a prior assumption of risks under the control of a department has been made;

(b) the use of insurance for other than the company's risks. Insurance is the undertaking by the insurer to indemnify another person or entity against loss or liability for loss in respect of specified perils or upon the occurrence of a specified event; or

(c) ensuring that appropriate insurance is carried in certain instances, such as through the specification or purchase of insurance by the government on behalf of others.

2.4 Financial analysis

The relative merits and cost-effectiveness of underwriting options and of loss control measures should be examined by assessing:

- the probable extent to which the company is directly or indirectly exposed financially;

- the degree to which the company can exert direct or indirect control over management of the risks and their underwriting;
- the direct and indirect costs of alternative underwriting options;
- the cost of investing in loss control measures compared with the probability of bodily injury or loss of life and the probable cost of damage to, or loss of, property;
- the net cost to the company, that is, whether underwriting costs rely on appropriations from tax revenues, or whether recovery could be used to offset the cost to the company, irrespective of the manner in which recovery may be allocated; and
- the merits, implications, and cost of an indemnification by the insurance.

Phase 3 - Containment

Containment is the third phase of risk management. Its primary purpose is to respond quickly to, and control, damaging incidents while they are happening, prevent the effects from spreading, and provide for continuation of the damaged service or function.

In effect, the containment phase entails implementation of all contingency plans developed earlier to minimize losses through the activation of emergency organizations, physical systems and procedures.

An important prerequisite to this phase is ensuring that contingency plans and systems are kept up to date and in good working order and, as far as possible, that people are trained and procedures are rehearsed.

Every department shall report on the contingency plan and systems and its working order and forward the same to Audit committee on annual basis.

Phase 4 - Compensation, restoration and recovery

4.1 General

Risk management, after the occurrence of a damaging incident, includes compensation, restoration and disaster recovery. Compensation is the settlement and payment of claims by or against the company or its employees. Restoration, an element of recovery, is the use of approved funding to repair or replace damaged, lost or stolen company property. In this phase, recovery entails completion of the longer-term measures initiated during containment to return operations to normal as soon as possible.

4.2 Investigation and assessment

Both compensation and restoration involve investigation and assessment. The company shall nominate the person to investigate and assess the damage and prepare its report and submit its report within 7 days to Audit committee.

Investigating the facts of a harmful or damaging incident has four purposes:

(a) establishing its cause;

(b) assessing the extent and value of damages and potential legal liability;

(c) providing a data-base in support of submissions for approval to pay claims; and

(d) providing feedback on the effectiveness of existing measures, and acting as a basis for establishing new or improved measures to prevent a recurrence.

An investigation report should be prepared on every incident, but its scope and degree of detail will vary with the complexities of the incident. Statements in the report should be restricted to the relevant facts and be as objective as possible. Items in the report could include, the incident, damages, the cause, expert advice and witnesses, comparable or previous settlements, sensitivity and precedent, claims, commercial and contractual, relevant statutes or other compensation and corrective action and risk management**.**

Appendix C - Special Provisions

The Risk Management Policy of the Company applies to all kinds and types of Risk. However, in case of following risk the Company may follow the following policy as well.

Risk Management in case of Commodity Price Risk:
For managing the Commodity Price Risk arising from fluctuation of price of commodities like manganese ore, coal, etc at domestic and international market, the management may carry out commercial negotiation with customers and suppliers to reduce such risk. The Company shall not enter into commodity hedging activities unless deemed necessary by Executive Director(s) or Chief Financial Officer of the Company.

The Management based on their intelligence and monitoring shall forecast Commodity prices and its movements to ensure that the Company is adequately protected from the market volatility in terms of price and availability of Commodities as may be required by the Company.

Risk Management in case of Foreign Exchange Risk:
For managing the Foreign Exchange Risk arising from fluctuation of foreign currency prices the management may resort to avail natural hedge arising out of Company's export and import. The variance between the Company's export and import shall be hedged to the extent considered necessary by Executive Director(s) and Chief Financial Officer of the Company.

The Management shall monitor the trends of foreign currency prices and its movements and based on their intelligence shall ensure that the Company is adequately protected from the foreign currency price fluctuations.

Risk Management in case of Cyber Threats:
Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems.

For managing the Cyber Threats the Management shall resort to the cost effective IT defensive security measures which may include web filtering, data storage encryption, installing antivirus engines, active patch management, installation of firewall, backup facility(ies), etc.

Management including Executive Director(s) shall decide the best way to incorporate and implement different types of security procedures in the Company and how to properly train Company staff to obviate cyber security threat.