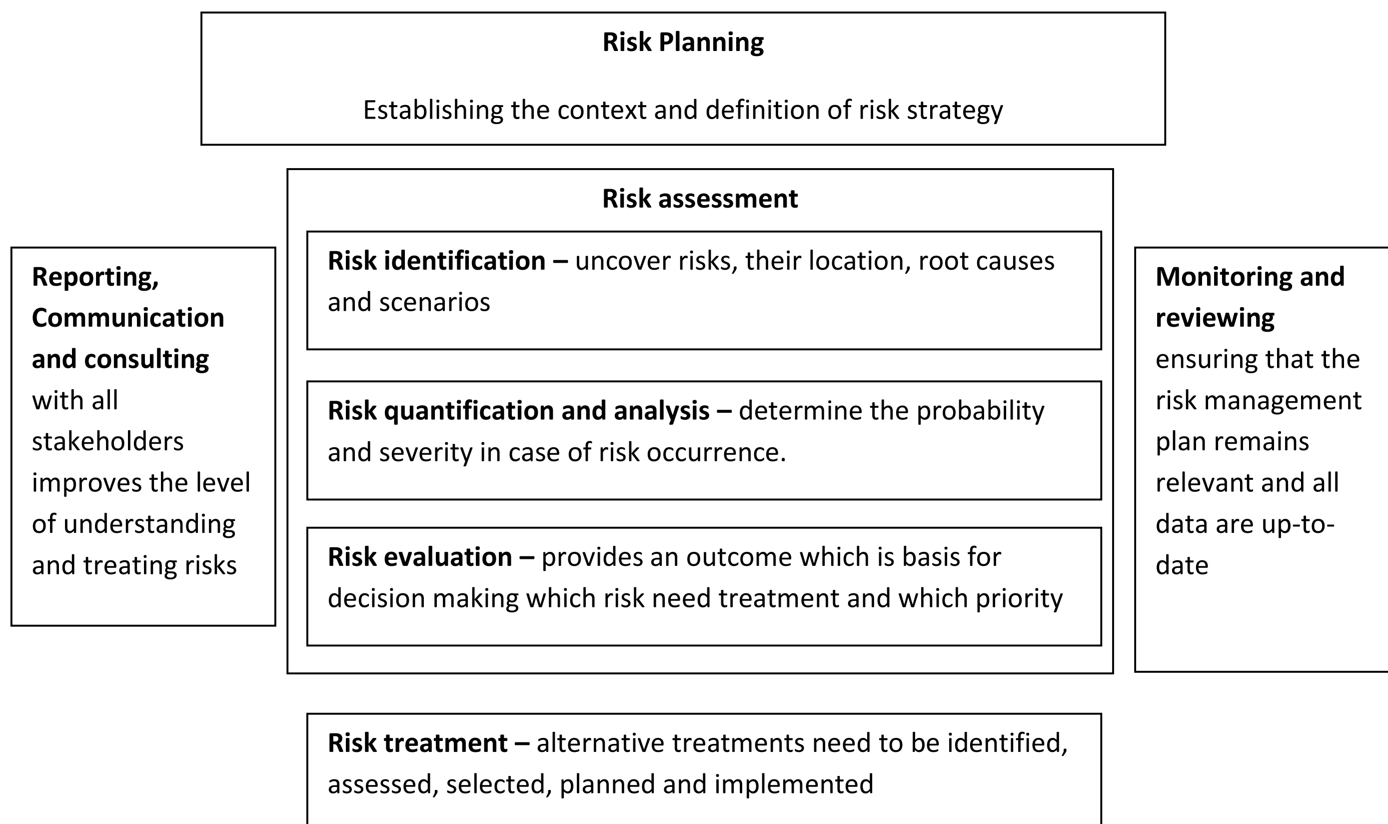
NRB INDUSTRIAL

Risk Management Policy

NRB Industrial Bearings Limited ('Board') is responsible for risk management, and for ensuring that robust internal controls are instituted to respond to changes in the business environment achieving objectives set out by the Board and being prepared for adverse situations or unplanned circumstances. The Board has put in place Risk Management Policy whose objectives are to optimize business performance; and to promote confidence amongst our stakeholders in the effectiveness of our business management process and our ability to plan & meet our strategic objectives and to protect shareholders value.

At an operational level, the respective functional managers are responsible for identifying and assessing risks within their area of responsibility; implementing agreed actions to treat such risks; and for reporting any event or circumstance that may result in new risks, or changes in existing risk profile.



NRB INDUSTRIAL BEARINGS LTD
REGD. OFFICE : DHANNUR, 2ND FLOOR, 15, SIR P.M. ROAD, FORT, MUMBAI - 400 001. INDIA\
TEL.: 9122 - 2270 4206 FAX : 9122 - 2270 4207
WEBSITE : http//www.nrbindustrialbearings.com
CIN : L29253MH2011PLC213963

Proper Risk Management Policy in place which assists the management to achieve the performance and profitability targets of the Company by:

1) Reducing earnings volatility to optimize risk-adjusted returns
2) Improving risk management competencies throughout the organization.
3) Promoting a pro-active approach to treating risks.
4) Allocation of adequate resources to mitigate and manage risks and minimize their adverse impacts.
5) Optimizing risk situations and bringing them in line with the risk appetite of the company.
6) Strengthening the risk management system through continuous improvement.
7) Reducing insurance premiums and optimizing transfer cost based on loss history and exposure level
8) Optimizing risk to your tolerance and appetite
9) Enhancing the health and safety of employees and customers
10) Improving business resilience.
11) To ensure compliances with applicable statutes, policies and management policies and procedures.

Risk Strategy

The definition of risk is the EFFECT OF UNCERTAINTY ON OBJECTIVES which can have negative or positive impacts. In this definition, uncertainties include events, which may or not happen, and uncertainties caused by a lack of information or ambiguity. The risk can be quantified as its probability (annual frequency of occurrence) multiplied by its severity (expected loss or gain). The risk is a semi-quantitative tool using orders of magnitude. A risk with definitions of probability (annual frequency) and severity must be defined in order to classify the identified risk scenarios.

A default risk matrix has been proposed:

- RISK LEVEL ranging from NO RISK to EXTREME RISK.
- PROBABILITY ranging from ALMOST IMPOSSIBLE to FREQUENT.
- SEVERITY ranging from NEGLIGIBLE to CATASTROPHIC.

RISK EXPOSURES

Hazard risk

Business interruption and net income exposure; Criminal exposure; Environmental liability exposure; General liability exposure; Machinery and boiler exposure; Natural disaster exposure; Product liability exposure; Property exposure.

Financial risk

Financial exposure; Credit exposure.

Operational risk

Fleet operation and marine exposure; Health and safety exposure; IT and Electronic exposure; Personnel and human capital exposure; Production, technological and R&D exposure; Project risk exposure; Supply chain exposure.

Strategic risks

Compliance, regulatory and legal exposure; Corporate governance and ethics exposure; Emerging risk exposure; Intellectual property exposure; Marketing and product management exposure; Reputational and brand exposure; Social, economic and political exposure.

RISK LEVEL DEFINITION: Management considers the definitions of risk levels based on the risk appetite in evaluating strategic alternatives, setting related objectives to treat related risks. A default risk matrix with predefined risk level definitions has been set up (ranging from NO RISK to EXTREME RISK). The risk level definitions should be adjusted to the risk appetite and risk tolerance limit of the company.

QUALITY OF CONTROL DEFINITION: The risk control definitions must be set which define the quality level of control processes in place to treat the different risk exposures. In this section, the risk control levels ranging from NONE to EXCELLENT can be defined. The state of the risk controls in place are used in the risk scenario analysis in order to validate its adequacy and if improvements are needed.

Risk Assessment and Treatment

Any given risk exposure can have either be a hazard or a speculative risk. Speculative risk is a situation in which either profit, loss or no loss is possible (e. stock investment). The decision to venture into a new market, purchase new equipment, diversify on the existing

product line, expand or contract areas of operations, commit more to advertising, borrow additional capital, etc., carry risks inherent to the business with a positive or negative outcome. Hazard risk occurs from an accidental loss including only the possibility of loss and no loss. Enterprise risk management should consider all types of risk an organization faces.

The following four main classes can be set-up even though some overlapping may occur:

Hazard risk: Business interruption exposure; Criminal exposure; Environmental liability exposure; General liability exposure; Health and safety exposure; Machinery and boiler exposure; Natural disaster exposure; Product liability exposure; Property exposure.

Financial risk: Financial exposure; Credit exposure.

Operational risk: Fleet operation and marine exposure; IT and Electronic exposure; Personnel and human capital exposure; Production, technological and R&D exposure; Project risk exposure; Supply chain exposure.

Strategic risk: Compliance, regulatory and legal exposure; Corporate governance and ethics exposure; Intellectual property exposure; Marketing and product management exposure; Reputational and brand exposure; Social, economic and political exposure.

Technology Obsolescence:

The Company strongly believes that technological obsolescence is a practical reality. Technological obsolescence is evaluated on a continual basis and the necessary investments are made to bring in the best of the prevailing technology

Fluctuations in Foreign Exchange:

The Company has limited currency exposure in case of sales, purchases and other expenses. It has natural hedge to some extent. However, beyond the natural hedge, the risk can be measured through the net open position i.e. the difference between un-hedged outstanding receipt and payments. The risk can be controlled by a mechanism of "Stop Loss" which means the Company goes for hedging an open position when actual exchange rate reaches a particular level as compared to transacted rate.

Risk identification involves determining the risk scenarios, which represent potential threats and opportunities to the company. Risk scenario analysis is essential for risk management to identify, analyze and prioritize the risks for the company. Scenario analysis is a process of analyzing possible future events by considering alternative possible outcomes. This may take form as a brain storming, and the judgment of field experts represents an

extremely valuable contribution. The identification of risk scenarios can be carried out, such as:

- Risk assessment questionnaires for hazard and operational risks
- Historical incident data for hazards risks
- Financial statements and accounting records for the identification of financial risks
- Flowcharts and organizational charts for operational risks
- Personal interviews with experts from different departments for all risk classes
- Risk workshops with upper management and board members for identification of strategic risks

As part of the risk scenario analysis one should undertake a Business Impact Analysis to identify secondary losses which will certainly occur. You need to identify what the impact to your business would be in the event of a disruption and determine basic recovery requirements. Critical activities may be defined as primary business functions that must continue in order to support your business.

You need to identify:

• Your critical business activities
• What the impact to your business would be in the event of a disruption
• How long could your business survive without performing this activity.

Risk treatment

Risk treatment actions need to be defined and prioritized and can be grouped into risk controlling (ex. prevent, reduce, transfer, exploit, avoid, duplicate, separate, diversify) and risk financing (ex. transfer, retention, insure). Risk treatment is the term used for taking action to modify risk. The recommendations of risk treatment aim to reduce the effect of uncertainty on the company's objectives. This means tackling anything that might lead to detrimental consequences together with whatever is beneficial in such a way that the result is a net benefit. The goal is both a decrease of the expected earnings at loss. To cover all key risk exposures, a company should establish a common risk treatment library which can be used by all business units in order to optimize the knowledge and human capital within the company. All risk treatment decisions should be evaluated in the context of risk return tradeoff analysis. It should also be evaluated if the recommendation increases the risk in another area when implemented.

Key Risk Indicators – "KRI"

A Key Risk Indicator, also known as a KRI, is a measure used in management to indicate how risky an activity is. KRI give us an early warning to identify potential event that may harm continuity of the activity/project. Key Risk Indicators for early warning of risk exposures

should be defined and monitored. A KRI can be identified by a root-cause analysis in order find the leading indicator triggering or initiating a risk event.

A company can monitor and manage its most important risk targets and tolerance limits through a set of key risk indicators (KRIs). KRIs can be expressed in a variety of units, according to the specific risk under discussion. Examples of KRIs can be number of calls to customer service related to product liability exposures, law suits filed against company related to general liability exposures, commodity price, and exchange rate related to financial exposures, change of number of competitors, company stock performance in relation to competitors related to marketing exposures.

KRIs can initiate action to mitigate developing risks by serving as triggering mechanisms for organizational units charged with monitoring particular KRIs.

Periodic Risk Management Report

A risk management report should contribute to sound risk management and decision making by the board and senior management. Risk management reports should cover all material risk areas within the organization and monitor changes and improvements such as:

- Risk assessment procedure
- Definition of Risk appetite
- Presentation of prioritized risks for the company locations (country, business unit, project based, per location, etc.)
- Risk Treatment Activities
- Insurance and risk transfer financing
- Losses and forecasts
- Allocation of cost of risk
- Risk management training topics and priorities
- Communication of risk
- Risk activities and risk priorities for the coming period

REVIEW

- This Policy shall be reviewed at least every year to ensure it meets the requirements of legislation and the needs of organization.

AMENDMENT

- This Policy can be modified at any time by the Board of Directors of the Company.

****