ELECTROTHERM (INDIA) LIMITED

RISK

MANAGEMENT

POLICY

ELECTROTHERM (INDIA) LIMITED
RISK MANAGEMENT POLICY

INDEX

ELECTROTHERM (INDIA) LIMITED
RISK MANAGEMENT POLICY

1.: LISTING AGREEMENT REQUIREMENT:

Clause 49 IV (C): Board Disclosures – Risk management

"The company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework."

2.: PREAMBLE:

Risk management is a rapidly developing discipline and there are many and varied views and descriptions of what risk management involves, how it should be conducted and what it is for.

Risk management is not just something for corporations or public organisations, but for any activity whether short or long term. The benefits and opportunities should be viewed not just in the context of the activity itself but in relation to the many and varied stakeholders who can be affected.

There are many ways of achieving the objectives of risk management and it would be impossible to try to set them all out in a single document. Therefore it was never intended to produce a prescriptive standard which would have led to a box ticking approach nor to establish a certifiable process.

3.: WHAT IS "RISK"?

Risk can be defined as the combination of the probability of an event and its consequences.

In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

Risk Management is increasingly recognised as being concerned with both positive and negative aspects of risk. Therefore this standard considers risk from both perspectives.

4.: RISK MANAGEMENT: SCOPE & SPHERE:

Risk management is a central part of any organisation's strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

The focus of good risk management is the identification and treatment of these risks. Its objective is to add maximum sustainable value to all the activities of the organisation. It marshals the understanding of the potential upside and downside of all those factors which can affect the organisation. It increases the probability of success, and reduces both the probability of failure and the uncertainty of achieving the organisation's overall objectives.

ELECTROTHERM (INDIA) LIMITED

RISK MANAGEMENT POLICY

Risk management should be a continuous and developing process which runs throughout the organisation's strategy and the implementation of that strategy. It should address methodically all the risks surrounding the organisation's activities past, present and in particular, future.

It must be integrated into the culture of the organisation with an effective policy and a programme led by the most senior management. It must translate the strategy into tactical and operational objectives, assigning responsibility throughout the organisation with each manager and employee responsible for the management of risk as part of their job description. It supports accountability, performance measurement and reward, thus promoting operational efficiency at all levels.

<u>4. a: External and Internal Factors:</u>

The risks facing an organisation and its operations can result from factors both external and internal to the organisation.

The diagram overleaf summarises examples of key risks in these areas and shows that some specific risks can have both external and internal drivers and therefore overlap the two areas. They can be categorized further into types of risk such as strategic, financial, operational, hazard, etc.

There are ranges of specific risks that have the potential to have an adverse impact on the business of the company.

Financial Risks:

The risk that a company will not have adequate cash flow to meet financial obligations.

The Board of Directors has adopted a number of financial risk policies which address market price risk, liquidity risk, credit risk and corporate and bank guarantees.

Business Risks:

The risk that a company will not have adequate cash flow to meet its operating expenses.

A range of policies and procedures deal with specific business risks such as Client concentration, Credit control, Geographical risks, Economic risks, Technology risks etc., including:

- Delegation of authority policy and guiding principles
- Capital investment tollgate processes
- Guide to Business Conduct
- Litigation Report

Legal & Statutory Risks:

Sometimes the Government changes the law in a way that adversely affects the company's position.

Political Risks:

The political risk that a country's government will suddenly change its policies.

Management Risks:

The risks associated with ineffective, destructive or underperforming management, which hurts shareholders and the company or fund being managed. This term refers to the risk of the situation in which the company and shareholders would have been better off without the choices made by management.

5.: RISK ASSESSMENT:

Risk assessment is defined as the overall process of risk analysis and risk evaluation.

Once risks have been identified, they must then be assessed as to their potential severity of loss and to the probability of occurrence. These quantities can be either simple to measure, in the case of the value of a lost building, or impossible to know for sure in the case of the probability of an unlikely event occurring. Therefore, in the assessment process it is critical to make the best educated guesses possible in order to properly prioritize the implementation of the risk management plan.

6.: RISK ANALYSIS:

6.a: RISK IDENTIFICATION:

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of the organisation, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification should be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. All associated volatility related to these activities should be identified and categorised.

Business activities and decisions can be classified in a range of ways, examples of which include:

• **Strategic -** These concern the long-term strategic objectives of the organisation. They can be affected by such areas as capital availability, sovereign and political risks, legal and regulatory changes, reputation and changes in the physical environment.

• **Operational -** These concern the day-today issues that the organisation is confronted with as it strives to deliver its strategic objectives.

• **Financial -** These concern the effective management and control of the finances of the organisation and the effects of external factors such as availability of credit, foreign exchange rates, interest rate movement and other market exposures.

• **Knowledge management -** These concern the effective management and control of the knowledge resources, the production, protection and communication thereof. External factors might include the unauthorised use or abuse of intellectual property, area power failures, and competitive technology. Internal factors might be system malfunction or loss of key staff.

• **Compliance -** These concern such issues as health & safety, environmental, trade descriptions, consumer protection, data protection, employment practices and regulatory issues.

6.b: RISK DESCRIPTION:

The objective of risk description is to display the identified risks in a structured format, for example, by using a table. The risk description table as mentioned below can be used to facilitate the description and assessment of risks. The use of a well-designed structure is necessary to ensure comprehensive risk identification, description and assessment process. By considering the consequence and probability of each of the risks set out in the table, it should be possible to prioritise the key risks that need to be analysed in more detail. Identification of the risks associated with business activities and decision-making may be categorised as strategic, project/ tactical, operational. It is important to incorporate risk management at the conceptual stage of projects as well as throughout the life of a specific project.

:TABLE: Risk Description:

1.	Name of Risk	
2.	Scope of Risk	Qualitative description of the events, their size, type, number and dependencies
3.	Nature of Risk	Eg. strategic, operational, financial, knowledge or compliance
4.	Stakeholders	Stakeholders and their expectations
5.	Quantification of Risk	Significance and Probability
6.	Risk Tolerance / Appetite	Loss potential and financial impact of risk Value at risk Probability and size of potential losses/gains Objective(s) for control of the risk and desired level of performance
7.	Risk Treatment & Control Mechanism	Primary means by which the risk is currently managed

		Levels of confidence in existing control Identification of protocols for monitoring and review
8.	Potential Action for Improvement	Recommendations to reduce risk
9.	Strategy and Policy Developments	Identification of function responsible for developing strategy and policy

6.c: RISK ESTIMATION:

Risk estimation can be quantitative, semi quantitative or qualitative in terms of the probability of occurrence and the possible consequence.

For example, consequences both in terms of threats (downside risks) and opportunities (upside risks) may be high, medium or low (see table 1.1). Probability may be high, medium or low but requires different definitions in respect of threats and opportunities (see tables 1.2 and 1.3).

TABLE 1.1: Consequences – Both Threat and Opportunities:

High	Financial impact on the organisation is likely to exceed Rs. x Significant impact on the organisation's strategy or operational activities Significant stakeholder concern
Medium	Medium Financial impact on the organisation likely to be between £x and £y Moderate impact on the organisation's strategy or operational activities Moderate stakeholder concern
Low	Financial impact on the organisation likely to be less that £y Low impact on the organisation's strategy or operational activities Low stakeholder concern

TABLE 2.2: Probability of Occurrence – Threats:

Estimation	Description	Indicators
High [Probable]	Likely to occur each year or more than 25% chance of occurrence	Potential of it occurring several times within the time period (for example- ten years). Has occurred recently.
Medium [Possible]	Likely to occur in a ten year time period or less than 25% chance of occurrence	Could occur more than once within the time period (for example – ten years). Could be difficult to control due to some external influences. Is there a history of occurrence?
Low [Remote]	Not likely to occur in a ten year period or less than 2% chance of occurrence	Has not occurred. Unlikely to occur.

TABLE 2.3: Probability of Occurrence – Opportunities:

Estimation	Description	Indicators
High [Probable]	Favourable outcome is likely to be achieved in one year or better than 75% chance of occurrence.	Clear opportunity which can be relied on with reasonable certainty, to be achieved in the short term based on current management processes.
Medium [Possible]	Reasonable prospects of favourable results in one year of 25% to 75% chance of occurrence	Opportunities which may be achievable but which require careful management. Opportunities for which the likelihood of success is low on the basis of management resources currently being applied.
Low [Remote]	Some chance of favourable outcome in the medium term or less than 25% chance of occurrence	Possible opportunity which has yet to be fully investigated by management. Opportunity for which the likelihood of success is low on the basis of management resources currently being applied.

6.d: RISK ANALYSIS METHODS AND TECHNIQUES:

A range of techniques can be used to analyse risks. These can be specific to upside or downside risk or be capable of dealing with both. (See Appendix, for examples).

6.e: RISK PROFILE:

The result of the risk analysis process can be used to produce a risk profile which gives a significance rating to each risk and provides a tool for prioritising risk treatment efforts. This ranks each identified risk so as to give a view of the relative importance.

This process allows the risk to be mapped to the business area affected, describes the primary control procedures in place and indicates areas where the level of risk control investment might be increased, decreased or reapportioned.

Accountability helps to ensure that 'ownership' of the risk is recognised and the appropriate management resource allocated.

7.: RISK EVALUATION:

When the risk analysis has been completed, it is necessary to compare the estimated risks against risk criteria which the organisation has established. The risk criteria may include associated costs and benefits, legal requirements, socio-economic and environmental factors, concerns of stakeholders, etc. Risk evaluation therefore, is used to make decisions about the significance of risks to the organisation and whether each specific risk should be accepted or treated.

8.: RISK REPORTING AND COMMUNICATION:

8.a: INTERNAL REPORTING:

Different levels within an organisation need different information from the risk management process:

The Board of Directors should:

- Know about the most significant risks facing the organisation
- Know the possible effects on shareholder value of deviations to expected performance ranges
- Ensure appropriate levels of awareness throughout the organisation
- Know how the organisation will manage a crisis
- Know the importance of stakeholder confidence in the organisation
- Know how to manage communications with the investment community where applicable
- Be assured that the risk management process is working effectively
- Publish a clear risk management policy covering risk management philosophy and responsibilities

Business Units Should:

- Be aware of risks which fall into their area of responsibility, the possible impacts these may have on other areas and the consequences other areas may have on them
- Have performance indicators which allow them to monitor the key business and financial activities, progress towards objectives and identify developments which require intervention (e.g. forecasts and budgets)
- Have systems which communicate variances in budgets and forecasts at appropriate frequency to allow action to be taken
- Report systematically and promptly to senior management any perceived new risks or failures of existing control measures

Individual should:

- Understand their accountability for individual risks
- Understand how they can enable continuous improvement of risk management response
- Understand that risk management and risk awareness are a key part of the organisation's culture
- Report systematically and promptly to senior management any perceived new risks or failures of existing control measures

8.b: EXTERNAL REPORTING:

A company needs to report to its stakeholders on a regular basis setting out its risk management policies and the effectiveness in achieving its objectives.

Increasingly stakeholders look to organisations to provide evidence of effective management of the organisation's non-financial performance in such areas as community affairs, human rights, employment practices, health and safety and the environment.

Good corporate governance requires that companies adopt a methodical approach to risk methodical approach to risk management which:

- Protects the interests of their stakeholders
- Ensures that the Board of Directors discharges its duties to direct strategy, build value and monitor performance of the organisation
- Ensures that management controls are in place and are performing adequately

The arrangements for the formal reporting of risk management should be clearly stated and be available to the stakeholders.

The formal reporting should address:

- The control methods – particularly management responsibilities for risk management
- The processes used to identify risks and how they are addressed by the risk management systems
- The primary control systems in place to manage significant risks
- The monitoring and review system in place

Any significant deficiencies uncovered by the system, or in the system itself, should be reported together with the steps taken to deal with them.

9.: RISK TREATMENT:

Risk treatment is the process of selecting and implementing measures to modify the risk. Risk treatment includes as its major element, risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer, risk financing, etc.

NOTE: In this standard, risk financing refers to the mechanisms (eg insurance programmes) for funding the financial consequences of risk. Risk financing is not generally considered to be the provision of funds to meet the cost of implementing risk treatment.

Any system of risk treatment should provide as a minimum:

- Effective and efficient operation of the organisation
- Effective internal controls
- Compliance with laws and regulations.

The risk analysis process assists the effective and efficient operation of the organisation by identifying those risks which require attention by management. They will need to prioritise risk control actions in terms of their potential to benefit the organisation.

Effectiveness of internal control is the degree to which the risk will either be eliminated or reduced by the proposed control measures.

Cost effectiveness of internal control relates to the cost of implementing the control compared to the risk reduction benefits expected.

The proposed controls need to be measured in terms of potential economic effect if no action is taken versus the cost of the proposed action(s) and invariably require more detailed information and assumptions than are immediately available.

Firstly, the cost of implementation has to be established. This has to be calculated with some accuracy since it quickly becomes the baseline against which cost effectiveness is measured. The loss to be expected if no action is taken must also be estimated and by comparing the results, management can decide whether or not to implement the risk control measures.

Compliance with laws and regulations is not an option. An organisation must understand the applicable laws and must implement a system of controls to achieve compliance. There is only occasionally some flexibility where the cost of reducing a risk may be totally disproportionate to that risk.

One method of obtaining financial protection against the impact of risks is through risk financing which includes insurance. However, it should be recognised that some losses or elements of a loss will be uninsurable eg the uninsured costs associated with work-related health, safety or environmental incidents, which may include damage to employee morale and the organisation's reputation.

Potential Risk Treatments:

Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories:

- **Transfer**
- **Avoidance**
- **Reduction**
- **Acceptance**

Ideal use of these strategies may not be possible. Some of them may involve trade offs that are not acceptable to the organization or person making the risk management decisions.

Risk avoidance

Includes not performing an activity that could carry risk. An example would be not buying a property or business in order to not take on the liability that comes with it. Another would be not flying in order to not take the risk that the airplane were to be hijacked. Avoidance may seem the answer to all risks, but avoiding risks also means losing out on the potential gain that accepting (retaining) the risk may have allowed. Not entering a business to avoid the risk of loss also avoids the possibility of earning the profits.

Risk reduction

Involves methods that reduce the severity of the loss. Examples include sprinklers designed to put out a fire to reduce the risk of loss by fire. This method may cause a greater loss by water damage and therefore may not be suitable. Halon fire suppression systems may mitigate that risk, but the cost may be prohibitive as a strategy.

Risk retention

Involves accepting the loss when it occurs. True self insurance falls in this category. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. War is an example since most property and risks are not insured against war, so the loss attributed by war is retained by the insured. Also any amounts of potential loss (risk) over the amount insured is retained risk. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

Risk transfer

Means causing another party to accept the risk, typically by contract or by hedging. Insurance is one type of risk transfer that uses contracts. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among construction or other contractors is very often transferred this way. On the other hand, taking offsetting positions in derivatives is typically how firms use hedging to financially manage risk.

10: MONITORING AND REVIEW OF THE RISK MANAGEMENT PROCESS:

Effective risk management requires a reporting and review structure to ensure that risks are effectively identified and assessed and that appropriate controls and responses are in place. Regular audits of policy and standards compliance should be carried out and standards performance reviewed to identify opportunities for improvement. It should be remembered that organisations are dynamic and operate in dynamic environments. Changes in the organisation and the environment in which it operates must be identified and appropriate modifications made to systems.

The monitoring process should provide assurance that there are appropriate controls in place for the organisation's activities and that the procedures are understood and followed.

Changes in the organisation and the environment in which it operates must be identified and appropriate changes made to systems.

Any monitoring and review process should also determine whether:

- The measures adopted resulted in what was intended

- The procedures adopted and information gathered for undertaking the assessment were appropriate
- Improved knowledge would have helped to reach better decisions and identify what lessons could be learned for future assessments and management of risks

11.: THE STRUCTURE AND ADMINISTRATION OF RISK MANAGEMENT:

11.a: RISK MANAGEMENT POLICY:

An organisation's risk management policy should set out its approach to and appetite for risk and its approach to risk management. The policy should also set out responsibilities for risk management throughout the organisation.

Furthermore, it should refer to any legal requirements for policy statements eg. for Health and Safety.

Attaching to the risk management process is an integrated set of tools and techniques for use in the various stages of the business process. To work effectively, the risk management process requires:

- Commitment from the chief executive and executive management of the organisation
- Assignment of responsibilities within the organisation
- Allocation of appropriate resources for training and the development of an enhanced risk awareness by all stakeholders.

11.b: ROLE OF THE BOARD:

The Board has responsibility for determining the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.

This may be through an executive group, a non-executive committee, an audit committee or such other function that suits the organisation's way of operating and is capable of acting as a 'sponsor' for risk management.

The Board should, as a minimum, consider, in evaluating its system of internal control:

- The nature and extent of downside risks acceptable for the company to bear within its particular business
- The likelihood of such risks becoming a reality
- How unacceptable risks should be managed
- The company's ability to minimise the probability and impact on the business
- The costs and benefits of the risk and control activity undertaken
- The effectiveness of the risk management process
- The risk implications of board decisions

11.c: ROLE OF THE BUSINESS UNIT:

This includes the following:

- The business units have primary responsibility for managing risk on a day to-day basis
- Business unit management is responsible for promoting risk awareness within their operations; they should introduce risk management objectives into their business
- Risk management should be a regular management-meeting item to allow consideration of exposures and to reprioritise work in the light of effective risk analysis
- Business unit management should ensure that risk management is incorporated at the conceptual stage of projects as well as throughout a project

11.d: ROLE OF THE RISK MANAGEMENT FUNCTION:

Depending on the size of the organisation the risk management function may range from a single risk champion, a part time risk manager, to a full-scale risk management department. The role of the Risk Management function should include the following:

- Setting policy and strategy for risk management
- Primary champion of risk management at strategic and operational level
- Building a risk aware culture within the organisation including appropriate education
- Establishing internal risk policy and structures for business units
- Designing and reviewing processes for risk management
- Co-ordinating the various functional activities which advise on risk management issues within the organisation
- Developing risk response processes, including contingency and business continuity programmes
- Preparing reports on risk for the board and the stakeholders

11.e: RESOURCES AND IMPLEMENTATION:

The resources required to implement the organisation's risk management policy should be clearly established at each level of management and within each business unit.

In addition to other operational functions they may have, those involved in risk management should have their roles in coordinating risk management policy/strategy clearly defined. The same clear definition is also required for those involved in the audit and review of internal controls and facilitating the risk management process.

Risk management should be embedded within the organisation through the strategy and budget processes. It should be highlighted in induction and all other training and development as well as within operational processes e.g. product/service development projects.

12.: APPENDIX:

RISK IDENTIFICATION TECHNIQUES – EXAMPLES:

• Brainstorming
• Questionnaires
• Business studies which look at each business process and describe both the internal processes and external factors which can influence those processes
• Industry benchmarking
• Scenario analysis
• Risk assessment workshops
• Incident investigation
• Auditing and inspection
• HAZOP (Hazard & Operability Studies)

RISK ANALYSIS METHODS AND TECHNIQUES – EXAMPLES:

Upside Risk:

• Market survey
• Prospecting
• Test marketing
• Research and Development
• Business impact analysis

Both

• Dependency modelling
• SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)
• Event tree analysis
• Business continuity planning
• BPEST (Business, Political, Economic, Social, Technological) analysis
• Real Option Modelling
• Decision taking under conditions of risk and uncertainty
• Statistical inference
• Measures of central tendency and dispersion
• PESTLE (Political Economic Social Technical Legal Environmental)

Downside risk

• Threat analysis
• Fault tree analysis
• FMEA (Failure Mode & Effect Analysis)