Elgi Equipment Limited

Enterprise Risk Management Framework

DOCUMENT CONTROL SHEET

Document Name	**: Risk Management Framework**
Issued By	**: Risk Management Steering Committee**
Approved By	**: Risk Management Committee**

PROPRIETARY NOTICE

Table of Contents

1. Introduction

Elgi Equipments Limited is a leading air compressor manufacturer with corporate office in Coimbatore, India. ELGi offers a complete range of compressed air solutions from oil-lubricated and oil-free rotary screw compressors, oil-lubricated and oil-free reciprocating compressors and centrifugal compressors, to dryers, filters and downstream accessories. The company's portfolio of products has wide application across industries.

ELGi has manufacturing facilities in India, Italy and US cater to various markets with products that suit the unique requirements of those markets. Warehouse facilities in Australia, Brazil, Middle-East and US support the growing sales, service and distribution network across the world.

The Company recognises the need to systematically manage and regularly review its risk profile at a strategic and operational level. The Company has so far identified legal and financial risks as the main threat to its business. With the changes in business environment and to help support the vision of the organisation, ELGi has identified the need to for an efficient, effective and demonstrable Enterprise wide Risk Management ('ERM') process within the company

The Enterprise Risk Management Framework and underlined policies are intended to enable the Company to adopt a defined process for managing its risks on an on-going basis. The objective of this document is to create an awareness about various risks associated with the business of ELGi. . This document sets out the infrastructure for risk management namely structure, process and, systems for effective management of risks within the organisation.

[Space left blank intentionally]

2. Regulatory Background

The following regulations below emphasis on the need for having a risk management framework in place for a listed manufacturing company in India:

- The Companies Act, 2013 requires the Board report on the development and implementation of risk management policy in the organization. It requires identification of the risks that may threaten the existence of the company. Audit committee is required to review the effectiveness of risk management system. It also enables evaluation of the risk management process to ensure that the system are robust and defensible
- LODR (Listing Obligations and Disclosure Requirements) Regulations, 2015 requires framing, implementation and monitoring risk management plan. The role and responsibility of the Risk Management Committee needs to be defined. The delegation, monitoring and reviewing of the risk management plan is to be reported to the committee. It also requires laying down of procedures to inform Board members about the risk assessment and minimization procedures.
- Kotak Committee Recommendations, 2018 extended the requirement of Risk Management Committee from the top 100 to the top 500 listed entities. It also increased the relevance of cyber security and other related risks

3. Risk Management Framework

This framework is intended to ensure that an effective enterprise risk management framework is established and an appropriate reporting mechanism for the same is embedded within the company.

The management shall periodically assess the impact of changes in external and internal environment on the pertinence of this framework. The Risk Management Committee (RMC) may approve necessary changes to this framework to align it with the prevailing business circumstances if it deems fit.

3.1 Applicability

This framework is applicable from the date as mentioned on the “Document Control Sheet” and applies to whole of the Company and includes all functions, departments, business units.

3.2 Risk Management Objectives

The Company is committed to implement an effective risk management system to:

- Improve its ability to prevent or timely detect risks;
- Monitor and escalate risks;
- Improve sharing of risk information;
- Provide flexibility for managing upside and downside scenarios.

3.3 Definitions

This Risk Management framework is formed around a common understanding of terminology used in this document:

a. Risk

Risk is a potential for loss or sub-optimization of gain caused by an event (or series of events) that can adversely affect the achievement of a company's business objectives.

b. Risk Management

The systematic process of identifying, analysing, and responding to risks that have the potential to generate adverse effects on the achievement of organizational objectives.

c. Risk Analysis

The process of determining the possibility of the risk event (likelihood) and the magnitude of their consequences (impact).

d. Risk Evaluation

The process used to determine risk management priorities by comparing the level of risk against predetermined standards, to generate a prioritized list of risk for further monitoring and mitigation.

e. Risk Assessment

Risk assessment is the combined process of Risk Analysis and Risk Evaluation.

f. Risk Category

Risks are classified into various categories for better management and control. Each risk category is appropriately defined for the purpose of common understanding.

g. Risk Appetite

Risk Appetite is defined as the amount of risk an entity is willing to take, given its capacity to bear risk burden and its risk philosophy.

(The Management shall, with the approval of the Board, define its Risk Appetite over a period of time, for each business area, after the process is implemented).

3.4 Structure

The Risk Management Structure, roles and responsibilities are set out in Chapter 4.

3.5 Risk Management Approach

The Risk Management Approach is explained in detail in Chapter 5.

3.6 Documentation

Appropriate documentation of each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be utilised.

The documentation will serve following purposes:

- to provide evidence of a systematic approach to risk identification and analysis;
- to provide a record of risks to support the development of a database of the Company's risks;
- provide accountability for managing the risks identified;
- facilitate continuous monitoring and review; and
- share and communicate risk management information across the Company.

The responsibility for documenting the individual risks has been assigned to the risk owners. Risk Owners are responsible for performing and documenting risk assessments and developing appropriate treatment plans.

The key documents pertaining to the risk management process that needs to be maintained by the Company are:

- Risk Register:
  Risk Register is a consolidated list of all risks that have been identified during the periodical review. It is the key document used to communicate the current status of all known risks and is used for management reviews, control and reporting. The consolidated risk register is owned by the Risk Management Committee ('RMC'). The functional risk registers will be owned by the respective Business units/ Functions.

- Risk Profile:
  Risk profile provides detailed description of the risk, existing controls and actions plans / controls for risk treatment.

[Space left blank intentionally]

4. Risk management organization

The organization structure for risk management is depicted through the flow chart below. Detailed notes on roles and responsibilities of each level follow.

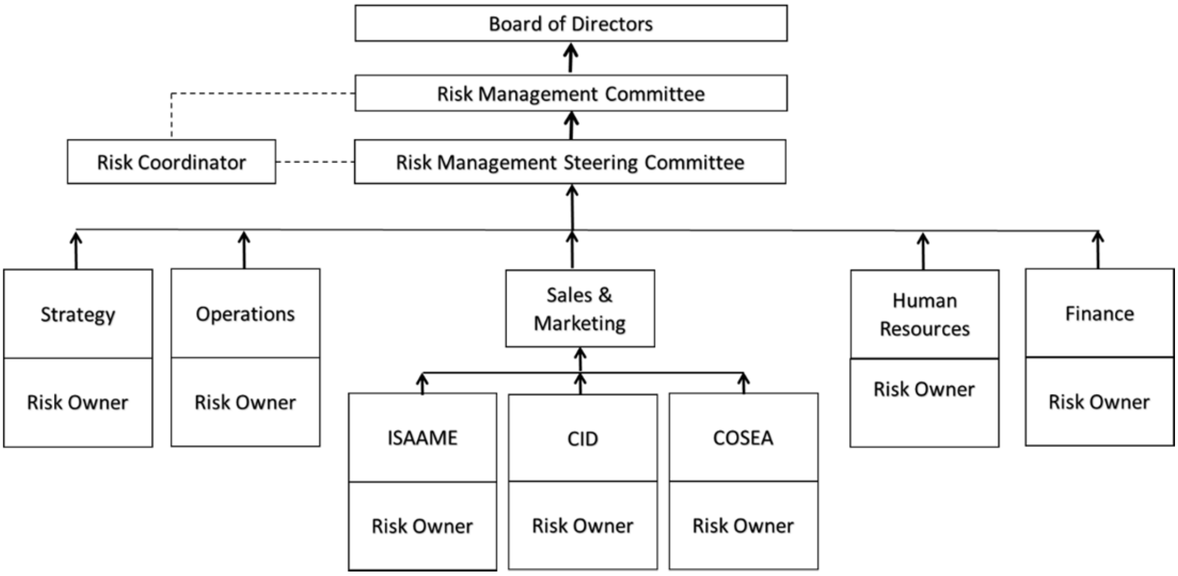


Fig.1 Overall Reporting Structure

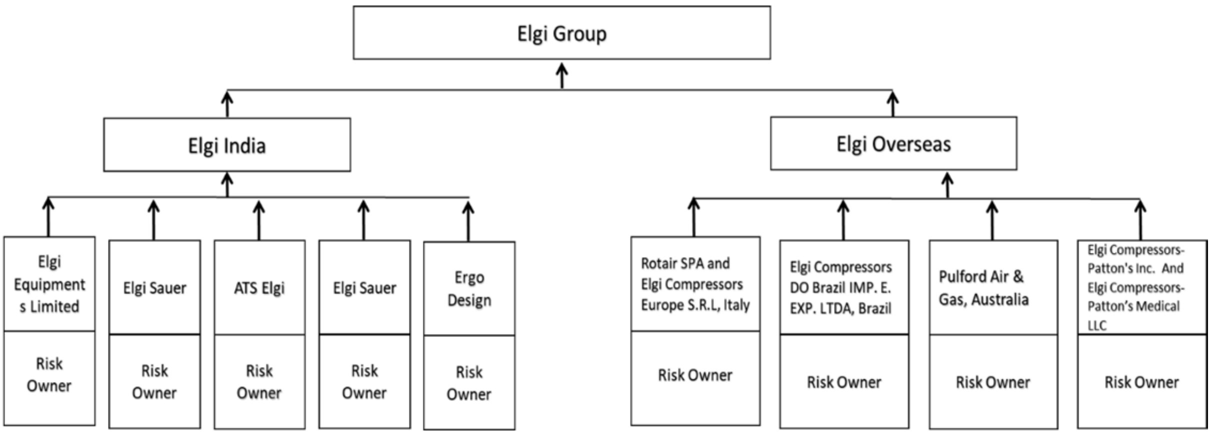


Fig.2 Entity wise Reporting Structure

[Space left blank intentionally]

4.1 Risk Management Committee (RMC)

The Chairperson and members of the RMC will be nominated by the MD. The committee shall be comprised of members from the senior management (including the heads of the risk management steering committees) and the Board. The chairperson of the committee may be an independent member of the Board.

The designated Risk Coordinator will coordinate activities relating to RMC. The RMC shall meet on a half yearly basis or more frequently if required for urgent matters. The Risk Coordinator will act as a convenor for the meetings of RMC and will maintain the reports of RMC's activities (agendas, decisions) and minutes of meetings (including attendance).

At a minimum, the RMC will perform the following activities:

- Periodic review of risks including status of mitigation plans
- Periodic review and update of consolidated risk register
- Periodic risk reports for the Board of Directors

4.2 Risk Coordinator

The Risk coordinator would be responsible as coordinator for risk management activity for the entire company. The Risk Coordinator would liaise with the function/BU risk coordinators to coordinate flow of information between them and the RMC. The Risk Coordinator would be responsible to ensure that meetings of the RMC are held as required, to review the risks identified. Risk Owners

4.3 Risk Owner

Risk Owners are individuals who understand the risk better and can contribute in mitigation of the same. Risk owners own, and therefore are deemed accountable for the effective management of risks assigned to them. Each risk will have one risk owner. The risk owners shall put in coordinated efforts to discuss the risks in detail, identify gaps in risk and controls, propose risk mitigation plans and review the implementation status of mitigation plans.

4.4 Roles & Responsibilities

The risk management roles and responsibilities will be as follows:

Role	**Responsibility**
Board of Directors	• Review and approve the risk management Policy for the company • Delegate monitoring and review of the risk management framework • Reporting to Shareholders in Board's report
Risk Management Committee (RMC)	• Lead the Risk Management initiative within the Company • Review and approve risk management framework • Review and approve the risk management report including selection of critical risks to be put before the Board • Oversee projects for effective implementation of risk mitigation strategies • Recommend training programs for staff with specific risk management responsibilities
Risk Management Steering Committee (RMSC)	• Develop and maintain risk management framework • Review and approve the risk registers for BU/functions • Advise business units and corporate functions on risk management framework • Spearhead risk management initiative within the Company

	• Monitor emerging issues and share best practices • Improve risk management techniques and enhances awareness • Set standards for risk documentation and monitoring • Recommend training programs for staff with specific risk management responsibilities
Risk Coordinator	• Liaise with the Risk Owners to coordinate flow of information and escalation of key risk issues/concerns before the RMSC • Ensure that meetings of the RMSC are held regularly and present updates / changes to Risk Assessment to the RMC on a periodic basis for approval • Prepare and maintain relevant documentation and RM Reports for the Company
Risk Owners	• Assess, review, monitor risks assigned to them. • Evaluate and validate the status of risk mitigation plans and propose additional controls. • Participate in review and monitoring of risks as part of the respective risk review committees.

5. Risk Management Process

5.1 Risk Identification

Comprehensive risk identification using a well-structured systematic process is critical, because a potential risk not identified is excluded from further analysis. Identification should include all risks whether or not they are under the control of the Company. Risks can be identified in a number of ways, viz:

- Structured workshops;
- Brainstorming sessions;
- Occurrence of a loss event;
- Review of documents.

All identified risks should be updated in a risk register. Risk registers should be periodically reviewed by the respective BU/Functions Head to ensure pertinence of the risks listed. Risks that would have ceased should also be closed appropriately. The risk coordinator should ensure that the risk register is reviewed and updated periodically.

5.2 Risk Assessment

The risks will be assessed on two-fold criteria. The two components of risk assessment are

(a) Likelihood of occurrence of the risk event and
(b) Magnitude of impact if the risk event occurs.

The combination of likelihood of occurrence and the magnitude of impact provides the inherent risk level. The likelihood and impact should be rated over a period of 12 to 18 months.

The magnitude of impact of an event, should it occur, and the likelihood of the event and its associated consequences, are assessed in the context of the existing controls. In determining what constitutes a given level of risk the following scale is to be used for likelihood:

Level	Descriptor
5	Very high likelihood
4	High likelihood
3	Moderate likelihood
2	Low likelihood
1	Very low likelihood

In determining what constitutes a given level of risk the following scale is to be used for impact:

Level	Descriptor
5	Very high impact
4	High impact
3	Moderate impact
2	Low impact
1	Very low impact

5.3 Risk Evaluation

For each risk, the average score for likelihood and impact shall be multiplied to arrive at a combined score. Example for Calculation of Group Score:

Rating of Risk X

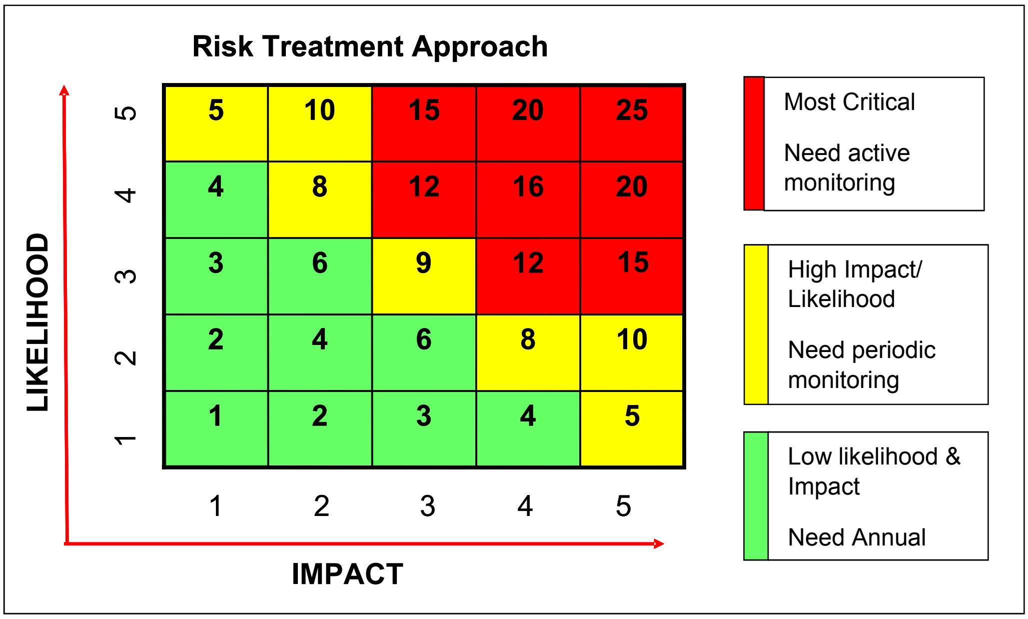
	Likelihood (A)	Impact (B)
Participant 1	2	5
Participant 2	3	5
Participant 3	4	5
Total	9	15
Group Score i.e. Simple Average (Total / No. of Participants)	3	5
Combined Score (Group Score A*Group Score B)	15	

The risk would be classified into one of the three zones based on the combined score.

- Risks that score within a red zone are considered "Critical / High / Unacceptable" and require immediate action plans to deal with the risk. (Average score 12 and above)

- Risks that score within the yellow zone are considered "Cautionary / Medium" where action steps to develop or enhance existing controls is also needed. (Average score in the range of 6 and less than 12)
- Risks that score within the green zone are considered "Acceptable / Low". (Average score less than 6).

Note: The boxes with value 5 have been included in the Yellow (Cautionary) zone due to very high likelihood/impact scores.



The output of a risk evaluation is a prioritized list of risks for further action

The objective of risk assessment and risk prioritisation is to assist the organization in prioritizing risk treatment strategies to ensure that appropriate attention is given to risks based on their criticality and that organisation resources are effectively utilized in managing these risks

5.4 Risk Treatment / Action Plan

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Treatment options may include: -

- *Avoidance* – Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- *Reduction* – Action is taken to reduce risk likelihood or impact, or both.
- *Sharing* – Sharing a portion of the risk by forming a joint venture
- *Transferring* - Includes purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.
- *Acceptance* – No action is taken to mitigate the risk or reduce the likelihood or impact

Action plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining policies, procedures, practices and processes in place that will ensure that existing level of risks are brought down to an acceptable level. In many cases significant risk may still exist after mitigation of the risk level through the risk treatment process. For risks considered to be “acceptable” risk profile will be developed with mitigation plan as accepted and no further actions required.

5.5 Escalation of risks

It is critical to institute an effective system of escalation, to ensure that specific issues are promptly communicated and followed up appropriately. After the risk is identified upward escalation of the same will be as below:

- BU/Function head to select risks to be escalated which primarily will be of following types:
  - Critical risks relevant to the unit/function wherein the complete mitigation is possible at unit/function
  - Critical interdependent risks wherein intervention of RMSC is required for smooth implementation of the mitigation plan. It is desired that risk owner at a business unit prepares risk mitigation plan at the unit/function level for such risks which may be considered by RMC for integrated response/mitigation plan.
- The Risk Management Steering Committee shall select risks to be escalated to RMC.
- RMC will review the risks submitted by RMSC and will identify and escalate risks to the Board

5.6 Risk Reviews

Ongoing review is essential to ensure that the management plans remain relevant. Factors, which may affect the likelihood and impact of an outcome, may change, as may the factors, which affect the suitability or cost of the various treatment options.

A risk review involves re-examination of all risks recorded in the risk register and risk profiles to ensure that the current assessments remain valid. Review also aims at assessing the progress of risk treatment action plans.

5.7 Risk closure:

A risk issue shall not be deleted from unit/ function level risk registers. A risk issue shall be closed after the approval of RMSC, due to any one of the following reasons:

- *Risk mitigated:* The risk is mitigated to the desired extent.
- *Risk not relevant:* The risk is not relevant/applicable to the respective Business Units/ Functions, due to change in external business environment
- *Risk transferred:* The risk has been transferred to some other Business Units Functions

6. Reporting

A report comprising of top critical risk areas (including mitigation plans) duly approved by the RMC, shall be placed before the Board. The format of such a report may be as suggested by the RMC.

On an annual basis, the Board would review the progress of risk management implementation (including areas such as training requirements, process improvisation etc.).

[Space left blank intentionally]

Annexure I: Assessment Parameters

a. IMPACT

Criteria	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Financial	Impact < 1 % of PBT	Impact within 1-3% of PBT	Impact within 3-5% of PBT	Impact within 5-10% of PBT	Impact >10% of PBT
Reputation	-Minimal local media attention -Short term recoverability of reputation	-Regional media attention -Loss of reputation for a moderate period of time	-Sustained negative regional media attention -Damage to Elgi's values and reputation/brand at limited circle and local level	-Negative national media attention -Substantial damage to Elgi's reputation/products/revenue at national level	-Sustained negative national media attention -Irreparable damage to Elgi's reputation/brand/values at the national/global level
Regulatory Compliance	-Minor technical non-compliance with no fine or prosecution	-Imposition of minor fine	-Regulatory breach leading to fines and prosecution of mid-level mgmt. of Elgi	-Regulatory breach and prosecution along with temporary suspension of business	-Prosecution by authority due to a regulatory breach, likely to result in imprisonment of the Sr mgt of Elgi with temporary prolonged suspension of operation

b. LIKELIHOOD

Criteria	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Likelihood/ Probability	Event could occur once in 10 years	Event likely to occur once in 5 to 10 years	Event expected to occur once in 5 years	Event may occur once in 3 years	Event certain to occur within a year