Classification: Internal

Thermax Limited

Enterprise Risk Management Policy

Revision History and Signoff			
Modification summary	Reviewed By	Approved By	Effective Date

Contents

1. OBJECTIVE:

Risk is inherent to a business and inevitably has an impact on the outcome of strategic decisions. The outcomes are determined by how a business is managed and, in turn they affect the management of business's operations. Risk Management is performing a series of activities designed to minimize this impact.

Enterprise risk is any risk that can have an impact (both negative as well as positive) on the achievement of the business's objectives and targets. The purpose of an Enterprise Risk Management policy is to develop processes to minimize the negative impacts of risks and to enhance the positive impacts. This Policy focusses on the negative impacts and does not cover the management of opportunities (the positive aspect of risks). These processes include identifying, analyzing, assessing, mitigating, monitoring, preventing, and governing any existing or potential risks. The systematic and proactive identification of risks and their mitigation enable effective and quicker decision-making, enable business continuity, and improve performance.

This document lays down the framework of Risk Management at Thermax Group and defines the policy for the same.

It seeks to identify risks and provide guidelines to define, measure, report, control and mitigate the identified risks.

2. SCOPE AND EXTENT OF THE POLICY:

This policy covers all activities within or outside the company that have a bearing on the company's existing and future performance. The policy shall operate in conjunction with other business/operating /administrative policies. This policy applies to all functions and units of Thermax Limited and its subsidiaries.

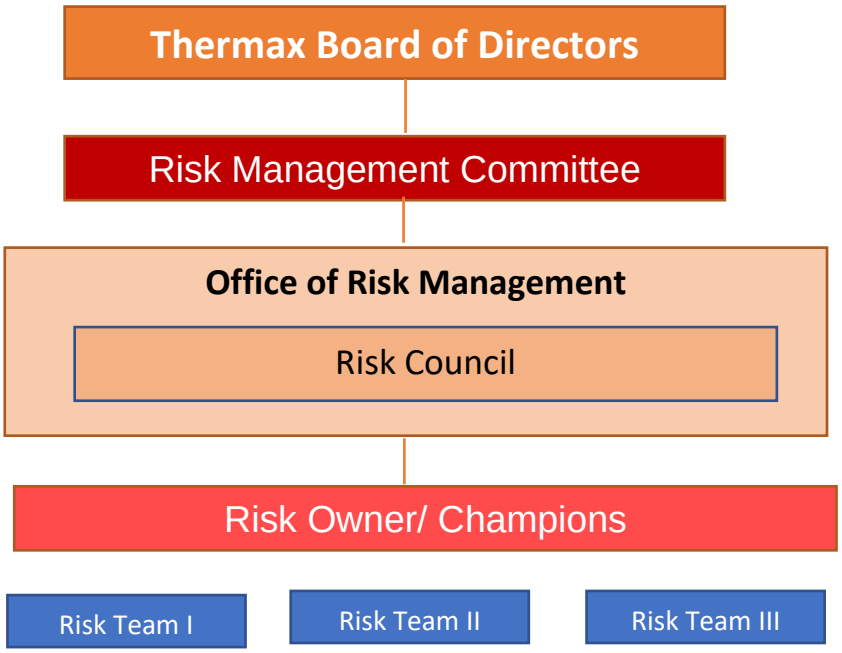
Materiality of impact shall govern all the provisions of this policy. For that purpose, the impact shall be judged with reference to plans and objectives both, financial and non-financial.

It shall be under the authority of the Board of Directors of the Company.

3. ERM GOVERNANCE STRUCTURE:

The Company's Board is responsible for oversight of company-wide management of risk and igniting & maintaining a culture of risk-consciousness within the enterprise. For that purpose, it has constituted a committee of board members called the Risk Management Committee.

Risk Management Policy will be implemented by the Risk Council whose role is set out in paragraph 4 below:



4. RISK MANAGEMENT COUNCIL

The company shall have a risk council whose membership shall comprise all members of the Executive Committee of Management, the Chief Internal Auditor and such others as may be co-opted. It shall be chaired by the Chief Finance Officer. Its role is:

- Framing for recommendation to the RM Committee the Risk Management Policy and Plans.
- Periodically reviewing this Policy.
- Evaluating significant risk exposures and assessing actions to mitigate them timely.
- Monitoring risks and risk management capabilities.
- Communicating to the functions concerned identified escalating risk.
- Reviewing crisis preparedness and recovery plans.
- Embedding a risk management culture.
- Supporting Risk Owners so that they can effectively monitor designated risks.
- Inculcating a common approach to risk, especially in each of the business segments.
- Developing a common risk language.
- Identifying inter-related risks and assessing the response to them.
- Assessing overall combined risks and the ability to deal with simultaneous unrelated risk events.
- Approving all external communications related to risks and their management (e.g., in the annual reports) before their recommendation to the Board or its committees.

The Risk Council shall meet once in a quarter or more frequently if the situation demands.

Risk Owners / Champions

- Due to an ever-changing external environment in which the company operates, there is a need to constantly monitor the changes that could impact the probability, impact & velocity of identified risks. Risk owners are responsible for monitoring and escalating any changes in risks.
- Risk mitigation plans have risk owners assigned across all business units to ensure accountability during implementation of mitigation measures. The mitigation plan implementation also forms part of the risk owners' KPIs.
- Progress of mitigation plans vis-à-vis targets also form part of reporting to the Risk Council & Risk Management Committee.
- Spreading awareness of risk, including through the participation of all stakeholders in identifying new risks and new methods of managing them.
- Encouraging use of a common risk language.
- Encouraging use of uniform risk processes and practices.

5. RISK MANAGEMENT PROCESS:

I. RISK IDENTIFICATION AND CATEGORIZATION:

- Some of the ways through which new risks can be identified are:
    - Brainstorming within a group of functional/process heads across business units
    - Interviews
    - Lists of risks found in similar businesses/areas
    - SWOT analysis
    - Research reports/market intelligence
    - Risk papers of Big 4 Accounting and other consulting firms
    - Risk factor disclosures in the annual reports of key business stakeholders
    - Crowdsourcing, involving all stakeholders in the Company.
    - Reports of not-for-profit global organizations, especially in the ESG field.

- Once risks are identified, they are categorized as one of the following: Existential, Strategic, Financial, Operational or Compliance.

RISK CATEGORIZATION:

Existential Risks:

- These are risks that, if they fructify, could threaten the existence of the company.

Strategic Risks:

- Risks that arise out of strategic plans or failure to take strategic decisions that could impact the result of the organization's objectives.
- Includes risks pertaining to innovation, market dynamics, mergers, acquisitions, divestments, failure to timely close or divest a business, the impact of the natural

environment on the company and of the company on the natural environment and corporate governance.

Financial Risks:

- Risks that arise out of uncertainties and fluctuations in the financial environment, thereby impacting the company's financial objectives.
- Includes risks pertaining to liquidity, credit, insurance and accounting & reporting

Operational Risks:

- Risks that are embedded in the company's own operations.
- Includes risks pertaining to project proposals, execution, reputation, post-sales service, supply chain and employees.

Compliance Risks:

- Risks flowing from the legal and regulatory structure.
- Includes risks pertaining to ethics, code of conduct, foreign laws, government regulations and advocacy.

II. RISK ASSESSMENT AND PRIORITIZATION:

- Identified risks are assessed and rated by key process heads/owners and key stakeholders based on Probability (Likelihood of the risk actualizing), Impact (financial/non-financial effect on the company) and Velocity (speed at which the risk exposure can impact the organization).
- The scale for probability, impact, and velocity is from 1 to 5 each, with 1 being 'rare' in probability, 'insignificant' in impact and 'Very Slow' in velocity, and 5 being 'certain' in probability, 'catastrophic' in impact and 'Immediate' in velocity. The table below details the rating scale for probability and impact.

	Impact	**Probability**	**Velocity**
1	Insignificant	Rare	Very Slow
2	Minor	Unlikely	Slow
3	Moderate	Possible	Moderate
4	Major	Likely	Rapid
5	Catastrophic	Certain	Immediate

- Risk ratings/Risk Criticality Scores are calculated in the following manner:

IMPACT X		PROBABILITY +		VELOCITY =		RISK CRITICALITY	
Impact Rating		Probability Rating		Velocity Rating		Risk Criticality Score	
5	Catastrophic	5	Certain	5	Immediate	High Risk	Risk with Risk Criticality score of >/= 20
4	Major	4	Likely	4	Rapid		
3	Moderate	3	Possible	3	Moderate	Medium Risk	Risk with Risk Criticality score of > 9 but < 20
2	Minor	2	Unlikely	2	Slow		
1	Insignificant	1	Rare	1	Very Slow	Low Risk	Risk with Risk Criticality score of </= 9

(Note: Risk Criticality Score has been re-calculated excluding velocity while determining top 10 risks.)

- The Risk criticality scores of the risks are compared to establish prioritization (risk with highest risk criticality score is given highest priority). The RM Council reviews all the identified risks and their scores to ensure no key risk has been under-prioritized.
- Risk is assessed at inherent (gross risk) and net risk (after considering risk mitigation plan) levels.

III. RISK STRATEGY AND MITIGATION PLAN:

- Mitigation strategies are discussed and finalized for each of the risks. Risk mitigation strategies could include risk avoidance, risk transfer, risk reduction, or risk retention.

- The mitigation plans are submitted to the Risk Management Committee on a quarterly basis by the Risk Council.

- Risk mitigation plans have risk owners assigned across all business units to ensure accountability during implementation of mitigation measures. The mitigation plan implementation also forms part of the risk owners' KPIs.

- Progress of mitigation plans vis-à-vis targets also forms part of quarterly reporting to the Risk Management Committee.

IV. RISK MONITORING:

- The Risk Council and Risk owners are responsible for monitoring and escalating any changes in risks including on the three parameters used for their assessment

- The risks and the effectiveness of the mitigation strategies are regularly reviewed by the Risk Management Committee and are reported to the Board.
- The following risks should be regularly monitored by the RM Council and RM Committee.

BUSINESS CONTINUITY PLAN

A Business Continuity Planning (BCP) involves creating a comprehensive plan to ensure continued operations during disruptions or crises. BCP's are required for risks corresponding to High Impact and High Velocity. They focus on minimizing the impact of various risks, such as natural disasters, supply chain disruptions, or other unforeseen events, on the organization's operations. The goal of a BCP is to minimise downtime, protecting assets, and maintaining stakeholder satisfaction.

CYBER SECURITY

A comprehensive cyber security plan for a company involves protecting the organization's diverse range of business units, assets, and data from cyber threats. Keeping in mind that cyber security is an ongoing process that requires continuous adaptation and improvement, there should be regular reviews and updates to the plan.

ESG RISK

ESG risk, refers to the potential adverse impacts or threats posed by environmental, social and governance (ESG) factors that could affect the organization's financial performance, reputation, and overall sustainability. ESG factors encompass a wide range of issues that can impact a company's operations, strategy, and long-term viability or can, in turn impact its stakeholders.

It is important to address ESG risks using double materiality, i.e., the impact on the business as also by the business because ESG defines the responsibility of the business to its stakeholders. Unlike other risks, this is an outward focused risk process.

By effectively managing ESG risks, the organization can benefit its stakeholders by mitigating its own negative impacts upon them as also providing them business solutions to handle negative environmental impacts that they may be exposed to.

6. RISK REGISTER:

A comprehensive enterprise-wide risk register, with details for each legal entity and for each business segment, will be maintained by the Risk Council that will be periodically updated with new risks and updates of existing risks.