Harsha Engineers International Limited

RISK MANAGEMENT POLICY AND FRAMEWORK

Date of Approval: 10/01/2022 Issuing Authority: Risk Management Committee and Board of Directors Effective Date: 10/01/2022 Date of Modification:1/05/2024 Effective Date of Modification: 1/5/2024

1. Foreword

1.1. Objective

The main objective of this Risk Management Policy and Framework ("**Policy**") is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business. In order to achieve the key objective, the Policy establishes a structured and disciplined approach to Risk Management in orderto guide decisions on risk evaluating & mitigation related issues. The Policy is in compliance with the Regulation 17(9) of SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended and provisions of Companies Act, 2013, as amended which requires the Company to lay downprocedures about risk assessment and risk minimization.

1.2. Applicability

This Policy applies to every part of Harsha Engineers International Limited's (the "**Company or Harsha**") business and functions.

2. Definitions

2.1. "**Company or Harsha**" means Harsha Engineers International Limited.

2.2. **"Chief Risk Officer or CRO"** means Chief Risk Officer of the Company and will be an officer at a level of Executive Director or GM.

2.3. **"Chief Sustainability Officer or CSO"** means Chief Sustainability Officer of the Company and will be an officer at a level of Executive Director or GM as Annexure 1.

2.4. **"Enterprises Risk Management Steering Committee or ERM Steering Committee or ERM" means** Enterprises Risk Management Steering Committee formed by the Company as per Annexure 1

2.5. **"Environmental, Social and Governance Steering Committee** or **ESG Steering Committee or ESG"** means Environmental, Social and Governance Steering Committee formed by the Company.

2.6. "**Risk**" means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may

or may not be avoidable by pre-emptive action.

2.7. "**Risk Management**" is the process of systematically identifying, quantifying, and managing all Risks and opportunities that can affect achievement of a corporation's strategic and financialgoals.

2.8. "**Risk Management Committee or RMC**" means the Risk Management Committee formed by the Board.

2.9. "**Risk Assessment**" means the overall process of risk analysis and evaluation.

3. Risk Management

Principles of Risk Management

3.1. The Risk Management shall provide reasonable assurance in protection of business value from uncertainties and consequent losses.

3.2. All concerned process owners of the company shall be responsible for identifying & mitigating key Risks in their respective domain.

3.3. The occurrence of Risk, progress of mitigation plan and its status will be monitored on periodicbasis.

4. THE RISK MANAGEMENT APPROACH AT HARSHA

Harsha has adopted a combined Enterprise Risk Management approach utilizing both top-down and bottom-up methods to identify and manage risks at the overall entity level.

This hybrid approach allows the Company for a strategic view of risks provided by the top-down perspective, coupled with a granular understanding of risks from the bottom-up perspective. This combination helps ensure alignment between enterprise goals and operational realities, promoting a balanced risk management strategy

5. RISK MANAGEMENT PROCESS

Objective of risk management process is to bring the inherent level of risk to a desired level of acceptable risk. In any company, inherent risk to an extent can be mitigated with the use of controls. Remaining risk called as residual risk can be mitigated with the use of effective treatment plans to bring the level of residual risk to a point which become acceptable to the company.

The risk management process adopted by Harsha. has been tailored to the business processes of the organization. Broadly categorizing, the process consists of the following stages/steps:

- Establishing the Context
- Risk Assessment (identification, analysis & evaluation)
- Risk Treatment (mitigation plan)
- Monitoring, review and reporting
- Communication and consultation

5.1 Establishing the Context

To effectively manage risks, it is crucial to establish the context, which serves as the foundation for the entire risk management process.

Establishing the External Context

External context refers to the broader external operating environment that influences an organization's risk management.

The external context can include, but is not limited to:

1. Political: Government policies, regulations, and shifts in political climate can affect an organization's operations and risk profile.
2. Economic: Macroeconomic conditions, such as inflation, exchange rates, and economic cycles, can impact an organization's financial stability and market position.
3. Technological: Advances in technology can present both opportunities and risks, with the potential to disrupt industries and alter an organization's competitive landscape.
4. Legal: New laws, amended regulations, and changing interpretations of existing legislation can introduce new risks or modify existing ones.
5. Environmental: Environmental concerns, including climate change, pollution, and resource scarcity, can impact an organization's sustainability efforts and reputation.

These factors, along with others such as market forces, dependencies, and key drivers, form the external context that organizations will consider while managing risk.

Establishing the Internal Context

To effectively manage internal risks, organizations should consider several aspects within the internal context

It is necessary to understand the internal context. This can include, but is not limited to:

1. Monitoring: Establish monitoring processes to track operations and detect issues early on.
2. Control Environment: Organize the workplace to minimize risk, ensuring safety equipment installation and implementing firewalls for cybersecurity.
3. Information and Communication: Develop regular reports and open communication channels between departments, workers, and managers to promote transparency and prevent miscommunication.
4. Risk Valuation: Determine the potential impact and likelihood of various risks, allowing for informed decision-making regarding risk mitigation efforts.

5. Objectives: Focus on the organization's strategic objectives, aligning risk management activities accordingly.
6. Structure: Understand the organizational structure, especially where certain risks are relevant based on the location, function, or division involved.
7. Systems: Analyze internal systems to identify potential risks and leverage quantitative data to inform risk assessments.

These internal context elements help organizations to identify, assess, and manage risks effectively, ensuring that risk management strategies are tailored to the organization's specific needs and objectives.

5.2 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation

Risk Identification

Identification of risks at various levels viz. employees, functional heads & senior management. Risk identification must begin with an understanding of the organizational objectives that the functional head are responsible for and also the strategies that have been adopted to achieve organizational objectives.

Risk analysis involves:

- consideration of the causes and sources of risk
- the trigger events that would lead to the occurrence of the risks
- the positive and negative consequences of the risk
- the likelihood that those consequences can occur

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.

Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties, other than the organization, that benefit from the risk. Decisions should be made in accordance with legal, regulatory and other requirements.

5.3 Risk Treatment

Risk treatment refers to the strategies employed to modify risks by reducing their likelihood and/or impact.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Following framework shall be used for risk treatment:

1. **Risk Avoidance**

This strategy involves completely avoiding a particular risk by resigning from performing specific actions or processes. It's used when the risk is deemed too high to mitigate, and the company chooses to pursue alternative actions with lower risks.

2. **Risk Reduction**

This strategy aims to take action to reduce the impact or likelihood of a given risk. It involves implementing safeguards or controls, such as fire-suppression systems or employee training, to bring the risk to an acceptable level.

3. **Risk Sharing/Transfer**

This strategy involves sharing the possibility of loss with others or transferring the risk to a third party, such as through insurance.

4. **Retention (accept and budget)**

Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is a viable strategy for 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. 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.

5.4 Monitoring and review

In order to ensure that risk management is effective and continues to support organizational performance, processes shall be established to:

- Measure risk management performance against the key risk indicators, which are periodically reviewed for appropriateness
- Periodically measure progress against, and deviation from, the risk management plan

- Periodically review whether the risk management framework, policy and plan are still appropriate, given the organizations' external and internal context
- Report on risk, progress with the risk management plan and how well the risk management policy is being followed
- Periodically review the effectiveness of the risk management framework.
- Structured scientific and analytical tools may be used for this purpose.

5.5 Communication and consultation

Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process. Therefore, plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk itself, its causes, its consequences (if known), and the measures being taken to treat it. Effective external and internal communication and consultation should take place to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required

6 RISK REPORTING

Reporting is an integral part of any process and critical from a monitoring perspective. Results of risk assessment need to be reported to all relevant stake holders for review, inputs and monitoring.

Approach for Implementation at Harsha :

The **Risk Owners** would be required to prepare risk evaluation reports on a quarterly and annual basis and submit the same to the CRO.

Quarterly Risk Register Review Report

The CRO and the Enterprise Risk Management & ESG Committee shall review the Risk Registers and identify any emerging/new risk and the existing control to mitigate that risk. They must ensure robustness of design and operating effectiveness of existing mitigating controls. If required, re–rate (existing risks)/rate (emerging risks) and prepare, implement action plan for risk treatment in situations where the existing controls are inadequate.

The Quarterly Risk Register Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings
- New key risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations

The Risk owner will be responsible for preparing and consolidating the report and submit the same to CRO. The Report shall be reviewed by the Enterprise Risk Management & ESG Committee.

Post the review and re-rating of the risks in Risk Register.

Annual Risk Database Review Report

The Enterprise Risk Management & ESG Committee shall review the respective Risk Database annually and evaluate if any changes are requisite to the impact and likelihood assigned to the risks and, re-rate the risks if applicable as per the guidelines and ensure effectiveness of design and operating effectiveness of existing mitigating controls.

The Annual Risk Database Review Report shall include:

- Risk rate movements, if any, along with reasons for changes in the impact and/or likelihood ratings
- New key risks identified, if any, along with risk criteria ratings and mitigation plans
- Status of the implementation of mitigation plans and reasons for any delays or non-implementations

The Risk Unit owner will be responsible for preparing and consolidating the report and submit the same to CRO. The Report shall be reviewed by the Enterprise Risk Management & ESG Committee**.** Post the review and re-rating of the risks in Risk Register.

The CRO would be required to prepare on a quarterly basis a report for the Enterprise Risk Management & ESG Committee detailing the following:

- List of applicable risks for the business, highlighting the new risks identified, if any and the action taken w.r.t the existing and new risks;
- Prioritized list of risks highlighting the Key strategic and operational risks facing the Company
- Root causes and mitigation plans for the Key Risk
- Status of effectiveness of implementation of mitigation plans for the Key Risks identified till date

The Enterprise Risk Management & ESG Committee would be required to submit report to the Risk Management Committee on a half yearly basis the following:

- An overview of the risk management process in place;
- Key observations on the status of risk management activities in the quarter, including any new risks identified and action taken w.r.t these risks;
- Status of effectiveness of implementation of the mitigation plan for key risks

7.Roles and Responsibilities

Board of Directors

The Board shall oversee the establishment and implementation of an adequate system of risk management across the company. Board shall comprehensively review the effectiveness of the company’s risk management system on an annual basis.

Risk Management Committee (RMC)

The RMC would review on Bi-Annually, the risk assessment & minimization procedures across the Company after review of the same by the Enterprise Risk Management & ESG Committee. RMC will assist the Board in independently assessing compliance with risk management practices. It will also act as a forum to discuss and manage key risks.

Enterprise Risk Management Steering Committee (ERM Steering Committee)

Key responsibilities of the ERM Steering Committee include:

- Identification of new risks.
- Monitoring the environment within which the risk exists to identify issues which may affect its impact on the Company or the likelihood of its arising
- Providing assurance that risk management policy and strategy of the Company are operating effectively
- Developing risk response processes and assessing adequacy of responses for the key risks identified through the risk management framework
- Ensuring the implementation of risk mitigation plans
- Monitoring the Key Risk Indicators (KRIs) of the Company.
- Preparation and Update of the Risk Register and Quarterly reports for the Board/Risk Management Committee.
- Present the quarterly risk management update report based on the inputs by the Chief Risk Officer (CRO) to the Risk Management Committee.

Chief Risk Officer

The Chief Risk Officer (CRO) plays a pivotal role in the oversight and execution of a company's risk management function. Working closely with the Board of Directors and Enterprise Risk Management & ESG Committee, the CRO is responsible for developing and implementing risk assessment policies, monitoring strategies, and implementing risk management capabilities. The CRO's ultimate objective is to help the Board and executive management to determine the risk-reward tradeoffs in the business and bring unfettered transparency into the risk profile of the business. The CRO works closely with the Risk Owners to identify risks and then evaluate and negotiate risk response plans based on cost-benefit analysis.

The CRO facilitates the execution of risk management processes and infrastructure as a key enabler to achieving the business objectives of the organization. Following are the key responsibilities of the CRO:

- Identification of new risks.
- Assist the Board and Enterprise Risk Management & ESG Committee to establish and communicate the organization's ERM objectives and direction;
- Assist management with integrating risk management with the strategy development process;
- Assist the Board and Enterprise Risk Management & ESG Committee to develop and communicate risk management policies.
- CRO will be the Coordinator of the Enterprise Risk Management & ESG Committee

- Facilitate enterprise-wide risk assessments, developing risk mitigation strategies where required, and monitoring key risks across the organization
- Monitoring the Key Risk Indicators (KRIs) of the Enterprise and Functional Level Key Risks on a continuous basis.
- Assists in establishing, communicating and facilitates the use of appropriate ERM methodologies, tools and techniques
- Works with business units to establish, maintain, and continuously improve risk management capabilities
- Enables effective alignment between the risk management process and internal audit
- the CRO will present the quarterly risk management report to the Enterprise Risk Management & ESG Committee.

Risk Owner

Risk owners will assess the risk by determining its probability of occurrence and its impact with an objective of reporting key risks to the CRO.

Key responsibilities of the Risk owners include:

- Identification of new risks
- Reviewing and discussing significant risk issues and ensuring horizontal collaboration in the development of mitigation strategies and the establishment of corporate priorities in resource allocation
- Reporting new risks or failures of existing control measures with remedial action to CRO & Enterprise Risk Management & ESG Committee.
- Keeping the risk registers and related action plans updated
- Consolidating the quarterly and annual risk register and database review reports and timely reporting to the CRO
- Submission of the quarterly risk register review report by the 15th day following the quarter end to the CRO.
- Submission of the annual risk register review report by the 30th day after the financial year end, to the CRO.
- Educating employees dealing with key activities in their unit of the risk management process
- Facilitating segment level and corporate level steering committee meetings
- Ensuring Management Action Plans developed in response to audit and evaluation recommendations adequately address the risks identified
- Providing management with information about the organization's controls and determining which controls should be in place to adequately lower the overall risk profile of various critical processes.

Risk Management Activity Calendar

Activity	Timelines
Risk Register Review report to be submitted by risk owners to the CRO	Quarterly By 15th day following the quarter end
Risk Register Review report to be submitted by risk unit owners	Annual By 30th day following the financial year end
Enterprise Risk Management & ESG Committee meeting to review the Corporate key risks/ reports from site/ units	Half Yearly
Review by Risk Management Committee	Half Yealy
Board meeting	Annually

8. Amendment

Any change in the Policy shall be approved by the board of directors ("**Board**") of the Company. The Board shall have the right to withdraw and / or amend any part of this Policy or the entire Policy, at any time, as it deems fit, or from time to time, and the decision of the Boardin this respect shall be final and binding. Any subsequent amendment/modification in the Companies Act, 2013 or the Rules framed thereunder or the Listing Regulations and/or any other laws in this regard shall automatically apply to this Policy.

9. Communication of this Policy

This Policy shall be posted on the website of the Company i.e.
https://www.harshaengineers.com/InvestorRelations/company-policies.php

Impact Criteria Definition

Impact	Profit Reduction/Loss in % per year at Standalone Level
1-Negligible	Less than Rs 50 Lakhs
2-Minor	Less than 1% of PAT
3-Moderate	Between 1% to 5%
4-Major	Between 5% to 10%
5-Severe	More than 10%

Note: It will change as per Management Decision

Likelihood Criteria Definition

Likelihood	Probability of Occurrence (in %)
1-Rare	Less than 5%
2-Not Likely	5% to 10%
3-Likely	11% to 50%
4-Highly Likely	51% to 90%
5-Expected	Over 90%

Note: It will change as per Management Decision

Likelihood	Impact				
	1-Negligible	2-Minor	3-Moderate	4-Major	5-Severe
1-Rare	Low	Low	Low	Low	Low
2-Not Likely	Low	Low	Low	Medium	Medium
3-Likely	Low	Low	Medium	High	High
4-Highly Likely	Low	Medium	High	High	High
5-Expected	Low	High	High	High	High

Note: It will change as per Management Decision

Risk Rating

Level of Risk	Action
High	High Risk. Top Management attention needed to develop and initiate mitigation plans in the near future
Medium	Moderate Risk. Functional Heads attention required
Low	Low Risk. Manage by routine procedure

Note: It will change as per Management Decision