VARROC GROUP

Enterprise Risk Management Policy

Version 2.0

(investors@varroc.com)

Contents

DEFINITIONS AND ABBREVIATIONS

Audit Committee – Committee of Board of Directors of the Company constituted under the provisions of the Companies Act, 2013 ("the Act") and the SEBI Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR).

Board – Board of Directors of VARROC ENGINEERING LTD.

ERM – Enterprise Risk Management. ERM is an on-going process involving the Company's Board of Directors, top / senior management, and other personnel. It is a systematic approach to setting the best course of action to manage uncertainty by identifying, analyzing, measuring, responding to, monitoring, and communicating risk issues / events that may have an impact on the Company's success achieving its business objectives.

RM Committee – Committee of Board of Directors of the Company constituted under the provisions of the Act and SEBI LODR.

RO / ERM Coordinator – Risk Officer or the Enterprise Risk Management Co-Ordinator the person responsible for coordinating and tracking the implementation of the ERM process and submitting reports to the Risk Management Committee, Audit Committee and the Board.

ERM Policy or the Policy – Enterprise Risk Management Policy. **VARROC ENGINEERING LTD or the Company** – Corporate, various Units / SBUs of VARROC ENGINEERING LTD and includes its Subsidiaries, Associate Company(ies), Joint Venture Company (ies) and Group Companies

Risk* – an event or activity that may have an adverse impact on the Company's ability to effectively execute its strategies and / or achieve its objectives. Risk can be defined as the probability of a threat exploiting vulnerabilities of business assets or processes or controls by occurrence of an event causing significant impact to the business operations and continuity and which could prevent the organisation from achieving its goals and objectives. *(* as defined in Standard on Internal Audit (SIA) 130 Risk Management issued by Institute of Chartered Accountants of India)***Risk Appetite** – the degree / level of risk, on a broad level, that the Company is willing to accept or take in pursuit of achieving its objectives. It may be Low, Medium, High, or Very High-risk appetite.

Risk Threshold – The maximum level of potential financial loss that the Company is ready to face in pursuit of its business objectives. It may be fixed as x% of the EBITDA as per the Annual Business Plan of the Company.

Risk Register – A record of all possible risks that a unit / corporate function may be exposed to in achieving the business objectives. It includes a listing of the risk events, potential impact, allocation of scores for likelihood and impact parameters (risk score), risk owners, risk mitigation plans, outcome, etc.

Risk Assessment Score – It is a rating score for each risk event derived by multiplying the likelihood score and the impact score. The Higher the score, the riskier the event is for the Company and vice versa.

Risk Owners – The persons who are directly responsible for identifying risk events, devising mitigation plans, and monitoring the implementation of mitigation plans to reduce the risks while achieving business objectives as set out in annual business plans. The Company and business unit heads are the primary risk owners and other officials are nominated by the Chairman & Managing Director (CMD) to monitor the various risk events and implement the risk mitigation plans.

1. INTRODUCTION

VARROC ENGINEERING Ltd ('the Company') is a Public Limited Company incorporated under the provisions of Companies Act, 1956 having its Registered Office at Plot No. L-4, MIDC, Waluj, Aurangabad – 431136 (M.S.)

In the evolving and fast-changing business environment, many risks exist in the Company's operating environment and continuously emerge on a day-to-day basis. The Company faces several financial risks like credit risk, liquidity risk, financial market risk, etc., and non-financial risks like strategic business and investment risks, production risks, operational risks, human resources risks, legal and compliance risks, technological and information security risks, integrity risks, etc. The Company also faces substantial market risks, reputational risks, political and security risks, and external risks in its operations. The Company's ability to create sustainable value is dependent on recognizing and effectively addressing key risks that exist in this environment.

Toward this end, the management felt the need for a comprehensive, enterprise-wide risk management (ERM) policy. Enterprise Risk Management (ERM) is a holistic approach to risk management that promotes an integrated and informed view of risk exposures across the Company.
The ERM framework aims to meet the following internal and external stakeholders' expectations:

a. Internal Stakeholder's expectations:
    - To protect value; and
    - To generate value to drive profitability and growth.

b. External Stakeholder's expectations:
    - To ensure regulatory and statutory compliance; and
    - To provide stability and business continuity.

To facilitate this, each of the business units / plants / divisions must adopt a robust risk management programme. The risk management programme does not aim at eliminating risks, as that would simultaneously eliminate all chances of rewards or opportunities. Instead, it is focused on ensuring that known risks are addressed proactively through a well-defined framework.

This risk management policy enumerates objectives, principles of risk management and a risk management framework – an overview of the risk management process, procedures and related roles and responsibilities in the following sections.

The vision of the Company in framing its risk management policy is to strategically optimize risk taking to achieve long term sustainable growth in earnings and shareholder value of the Company.

2. OBJECTIVES

The ERM Policy is designed to manage risk within the risk threshold established by the Board while also providing reasonable assurance that strategic and operational objectives will be met.The objectives of risk management are to:

a. Consolidate and improve all the risk management practices currently followed by the Company and create common framework for managing risks.
b. Understand and better manage the uncertainties that may impact business performance;
c. Contribute to safeguarding the Company's value and the interests of shareholders;
d. Ensure that sound business opportunities are identified and pursued without exposing the business to an unacceptable level of risk; and
e. Improve compliance with good corporate governance guidelines and practices as well as laws

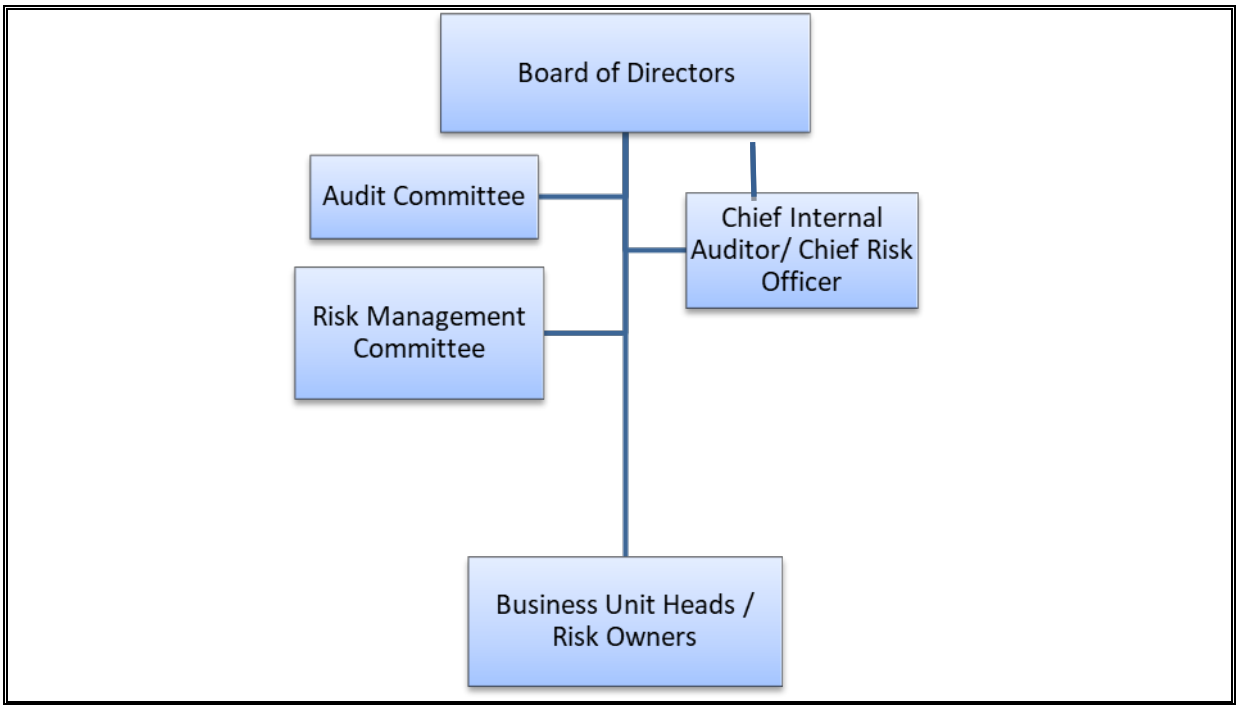
and regulations.

3. SCOPE

This ERM Policy document covers the enterprise-wide risk management aspects of all Business Units / Plants of the VARROC Group.

4. GOVERNANCE STRUCTURE

The ERM Governance structure would involve the following bodies / officials.



5. ROLES & RESPONSIBILITIES

5.1 Board of Directors

The Board of Directors of the Company shall undertake oversight of the program, including:

a. Define the role and responsibility of the RM Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit such function shall specifically cover cyber security; and

b. Approve and review the ERM Policy;

c. Articulate and periodically review the risk appetite and risk tolerance thresholds of the Companyd. Review and consider recommendations of Audit Committee and the RM Committee

5.2 Audit Committee of the Board

a. Monitor the implementation of ERM policy and advise on strategic processes for risk control;

b. Review the Company level risk report, suggest interventions, mitigation plans as required;

c. Evaluation of internal financial controls and risk management systems; and Review the

internal audit reports to assess the effectiveness of risk management processes and internal controls.

5.3 RM Committee:

To formulate a detailed risk management policy which shall include:

a. A framework for identification of internal and external risks specifically faced by the listed entity, including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee.
b. Measures for risk mitigation including systems and processes for internal control of identified risks.
c. Business continuity plan.
d. Ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with the business of the Company;
e. Monitor and oversee implementation of the ERM policy, including evaluating the adequacy of risk management system;
f. Periodically review the ERM policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
g. Keep the Board of Directors informed about the nature and content of its discussions, recommendations, and actions to be taken;
h. Appointment, removal, and terms of remuneration of the Chief Risk Officer shall be subject to review by the RM Committee.
i. Coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the board of directors.
j. Any other role or responsibility as may be delegated by the Board of Directors from time to time.
k. The Risk Management Committee shall be apex body to approve the risks, its mitigation plan, and the future course of action in this regard. While discharging the above-mentioned roles and responsibilities, the Committee can seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it considers necessary.

5.4 Chairman & Managing Director (CMD)

a. Inculcate the culture of Risk Management in all spheres of activity amongst the top and senior management of the Business Units;
b. Suggest mitigation measures to Unit CXOs / Risk Owners and monitor implementation;
c. Nominate functional risk owners at the corporate level, monitor the risk profile of corporate functions and oversee the implementation of risk mitigation plans.

5.5 Business Unit Level CXOs / Plant Heads / Functional Heads (Risk Owners)

a. Inculcate the culture of risk management in all spheres of activity amongst the senior management and all the operating personnel at the business unit level and plant level;
b. Drive the entire ERM programme at the Unit/Plant Level in consultation with the CMD;
c. Nominate other senior officials, as required, to be the risk owners for various functions;
d. Validate the Risk Register at periodic intervals and submit periodic reports to the RM Committee and the Audit Committee of the Company through the designated Risk

Officer; and

e. Drive the implementation of risk mitigation plans to improve the Risk Scores.

5.6Chief Risk Officer (CRO)

The Chief Internal Auditor will act as Chief Risk Officer of the Company. The roles and responsibilities of the CRO are as follows:

a. Follow-up with the risk owners at the Business Unit/Plant Level for the updation of the risk register at periodic intervals and as and when there is any major change in the perception of risk events that warrants the attention of the top management;

b. Track and monitor the implementation of risk mitigation measures both at the unit level and across corporate functions;

c. Report the unit-wise risk assessment score at periodic intervals to the Audit Committee and the Board; and

d. Coordinate the entire ERM programme at the Company Level and consolidate the risk registers.

5.7Chief Internal Auditor of the Company

a. Conduct a risk-based audit of various functions across all business units/plants in the context of the risks identified in the risk register;

b. Submit periodic internal audit reports to the Audit Committee of the Company;

c. The core role of ERM is to provide objective assurance to the Board that the major business risks are being managed appropriately and that the risk management and internal control framework is operating effectively.

6. RISK IDENTIFICATION

6.1 Business Unit/Plant Heads shall validate a Risk Register with details of various possible risk events that may impact the business in achieving the business plans / objectives.

6.2 The Risks shall be identified under following broad categories –:

Risk Category	Description
Strategic Risk	**Risk associated with the competitive positioning of the business and our ability to respond in a timely manner to changes in the competitive landscape. This includes risks to the value of the Company brand.**
Operational Risk	**The risk of loss resulting from various operations of the Company, inadequate or failed internal processes, people and systems or from external events.**
Financial Risk	**Risk of loss resulting from participation in credit and financial markets. This includes the risk of loss from refinancing issues and changes in financial market variables that impact revenue, expenditure, EBITDA and** the **valuation of** assets **and liabilities.**
Compliance Risk	**Risk emanating from non-compliance of various statutory, regulatory, legal provisions and contractual obligations leading to penalties, litigation etc. This includes adherence to internal policies and industry standards.**
Cyber Security Risk	Delivering end-to-end mobility solutions requires a number of critical enablers, including IT and digitization. **Probability of exposure, loss of critical assets and sensitive information, or reputational harm** because of **a cyber-**

Risk Category	Description
	attack or breach within an organization's network including **risks associated with data security, information privacy**.
Sustainability Risk	**An environmental, social or governance event or condition that, if it occurs, could cause an actual or a potential material negative impact on the value of the investment. If a sustainability risk associated with an investment materialises, it could lead to the loss in value of an investment.**

6.3 Risk identification shall be done under all the Business Units/Plants/functions of the Company. The broad functions are listed below:

a. Project Implementation;
b. Finance & Accounting;
c. Commercial & Raw Materials;
d. Marketing & Sales;
e. Production, Operations & Maintenance;
f. HSE, Security & Insurance;
g. Legal & Compliance;
h. Human Resources;
i. Information Technology; and

6.4 Corporate Social Responsibility activities. The Risk Register shall have columns for category of Risk, Risk Event, Likely impact (qualitative and quantitative), Score for Probability or Likelihood of occurrence, Score for Impact, Risk Rating Score, Functional Risk Owner, if any, Mitigation Measures, Outcome etc.

6.5 The guidance for assigning the rating scale for likelihood and impact is given in the next section on "Risk Measurement".

6.6 A sample Risk Register for illustration purpose is given below.

	ABC Ltd		Unit / Function Name			As on	01-01-16				
Sr. No.	Risk Event	Risk Category	Functional Category	Impact	Description	Risk Owner	Likelihood of occurrence	Impact if occurs	Risk Score (H*I)	Mitigation Plan	Result of Implementation
A	B	C	D	E	F	G	H	I	J	K	L
1									0		
2									0		
3									0		
4									0		
5									0		
6									0		
7									0		
8									0		
9									0		
10									0		

@	Category of Risk	Strategic
		Operational
		Financial
		Compliance
		Cyber Security
		Sustainability

#	Likelihood of occurrence (Rating Scale)	1 – Remote
		2 – Unlikely
		3 – Possible
		4 – Likely
		5 - Almost Certain
*	Impact if occurs (Rating Scale)	1 – Insignificant
		2 – Minor
		3 – Moderate
		4 – Major
		5 – Extreme

7. RISK MEASUREMENT

7.1 The likelihood of a risk event occurring may be measured on a scale of 1 (remote) to 5 (Almost certain). This 'Likelihood Score' is mostly a qualitative measure based on the judgement of the risk owners. On the happening of a risk event, the consequences or impact of such risk events on the organisation may be qualitative and / or quantitative in nature. The Risk Owners need to assign an impact score for each risk event on a scale of 1 (Insignificant) to 5 (Extreme).

7.2 The guidance for assigning the "Likelihood Score" or "Probability Score" is as below.

Likelihood of Occurrence	Probability	Occurrence in future	Occurrence in the past	Rating Scale
Almost Certain	Over 75%	Will be almost a routine feature within the immediate next year	Similar instances have commonly occurred in the past years	5
Likely	50% to 75%	May arise several times within the immediate next year	Similar instances have occurred several times in the past years	4
Possible	20% to 49%	May arise once or twice within the immediate next year	There have been a few similar instances in the past years	3
Unlikely	10% to19%	May occur once or twice in the next few years	There have been one or two similar instances in the last 2 to 5 years	2
Remote	Up to 9%	Highly unlikely to occur in the next few years	Similar instances have never occurred in the past	1

7.3 The guidance for assigning the "Risk Impact Score" is as below. (Any of the three conditions)

Likely Impact – Nomenclature	Likely Financial Impact on EBITDA of the Unit	Likely Reputational Impact	Likely Compliance Impact	Rating Scale
	A	B	C	
Extreme	Loss of over 10% of EBITDA	Extreme adverse public exposure / brand image in the long term (over a year) leading to deterioration in the credit rating.	Loss of business license/ conditions imposed by the regulator which would impair Company's operations in the long term (over a year) Criminal offence by director or manager. Severe/ Gross negligence in complying with the regulations / laws; hefty penalty.	5
Major	Loss of over 5% and up to 10% of EBITDA	Negative public exposure / brand image in the long term (over a year) leading deterioration in the credit rating	Loss of business license / conditions imposed by the regulator which would impair Company's operations for about a year; Criminal offence by Director or Manager. Major negligence in complying with the regulations / laws; sizeable penalty.	4
Moderate	Loss of over 2% and up to 5% of EBITDA	Negative public exposure/ brand image with short term (less than a year) impact	Conditions imposed on business license by the regulator for a short period (less than a year); Civil offence by Director or Manager; Negligence in	3

Likely Impact – Nomenclature	Likely Financial Impact on EBITDA of the Unit	Likely Reputational Impact	Likely Compliance Impact	Rating Scale
			complying with the regulations / laws; Moderate penalty	
Minor	Loss of over 1% and up to 2% of EBITDA	Minor Incident reported in media without any negative public exposure.	Civil offence by employee; Warning by the regulator; Minor penalty	2
Insignificant	Loss of up to 1% of EBITDA	Minor and segmented business partner concerns / incidents, but not reported in media	Caution letters from the regulator; insignificant penalty.	1

8. RISK APPETITE AND THRESHOLD

8.1 A certain level of risk is inherent in all the business activities of the Company. Risk appetite is the tendency of the Company towards taking risks. The Board is responsible for determining the acceptable level of risk based on the trade-off between assumed risk versus the expected value of the opportunities.

8.2 Currently, the Company's Risk Appetite is set to be at Medium level. The Risk Appetite shall be reviewed periodically by the Audit Committee in line with business objectives.

8.3 The overall risk threshold limit for the company is currently fixed at a potential loss of 10% of EBITDA as projected in annual business plan. If the potential impact of various medium to high-risk events of any business unit or Plant exceeds this threshold limit, the Business unit/plant CXOs shall escalate the matter to CMD to initiate top priority measures to reduce the impact.

The Risk Scores are defined as below:

Risk Score = Likelihood Score X Impact Score	Description of Consequences	Actions Required

Very High Risk (20 to 25)	a. Extreme financial loss b. Extreme threat of discontinuity in critical business operations c. Extreme reputational impact	Requires essential, immediate and top priority allocation and organization of resources to manage/mitigate the risk; Establish plans and counter measures.
High Risk (15 to <20)	a. High financial loss b. High threat of discontinuity in critical business operations c. High reputational impact	Requires priority allocation of resources for management and/or mitigation; Establish plans and counter measures.
Moderate Risk (10 to <15)	a. Medium level of financial loss b. Medium threat of discontinuity in critical business operations c. Medium to low reputational impact	Allocation of adequate resources for study is desirable; Risk events should be continuously monitored for increases in impact or likelihood.
Low Risk (5 to <10)	a. Low level of financial loss b. Low threat of discontinuity in business operations c. Low to negligible reputational impact	Generally, does not require action, but should be reviewed periodically to detect any possible worsening.
Very Low Risk (1 to <5)	a. Negligible financial loss b. Negligible threat of discontinuity in critical business operations c. Negligible reputational impact	No action required. May be reviewed periodically.

Risk Rating Score Matrix

Colour Code for Risk Rating –

Red – Highest Level of Risk Rating
Brown – High Level of Risk Rating
Pink – Moderate Level of Risk
Rating Yellow – Low level of Risk
Rating Green – Lowest level of Risk
Rating

9. RISK MITIGATION RESPONSE

9.1 Risk mitigation responses may be in the form of avoiding, accepting, reducing or sharing Risk.

9.1.1 Avoiding Risk – Here, the activity would not be undertaken, and any opportunity associated with it would be lost.

9.1.2 Accepting Risk – Here, the Company has no immediate mitigation measure to prevent the event from occurring or reduce the impact and hence takes the potential impact in books of accounts.

9.1.3 Reducing Risk – Here, risk mitigation measures are applied, and attempts are made to reduce the likelihood of occurrence or the impact of the occurring risk events. Unit insurance, Personnel Insurance, appropriate hedging of market risk exposures, adherence to SOPs, etc., are some of the tools to reduce risk.

9.1.4 Sharing Risk – Here, attempts are made to share the risk with the counterparties to the transactions through negotiations.9.2 The Business Unit/Plant CXOs and other Risk Owners shall actively devise mitigation plans under the guidance of CMD and/ or Business Unit/Plant Heads and other Top Management personnel to ensure that the Risk thresholds are not breached.

9.3 In devising the mitigation plans, the Company / Units shall be guided by the following:

9.3.1 strategic goals and objectives:

a) Manage risks that support businesses which are central to the enterprise strategy;
b) Based on the risk assessments, aim to reduce, or avoid risks that are not central to the achievement of the enterprise strategies / objectives.

9.3.2 Mitigation of exposure to significant loss from businesses, products, processes, or other events:

a) Follow a rigorous due diligence process for various commercial transactions;
b) Ensure that the investment and valuation processes are robust;
c) Funding plans and projections are performed at regular intervals and reviewed frequently to minimize funding surprises.

9.3.3 Reputational considerations:

(a) VARROC protects its value and reputation by operating with excellence and applying a disciplined approach to risk management, governance, and internal control, including compliance with all regulatory and statutory provisions;

(b) VARROC strives to maintain the highest level of professionalism, integrity, ethical behaviour and reputational standards.

9.3.4 The CMD, the Business Unit/Plant Heads, CXOs and Risk Owners shall closely monitor the high-risk events and ensure timely allocation of adequate resources to manage and reduce the likelihood or impact of such high-risk events.

10 **REPORTING REQUIREMENTS**

10.1 Business Unit/Plant Head/Corporate function, CXOs to report the updated Risk Register to the CMD at periodic intervals and whenever escalation is required to the Audit Committee/RM Committee/Board.

10.2 Such Business Unit/Plant Level report reviewed by the CMD shall be presented to the RM Committee and if required to the Audit Committee/Board by the CRO.10.3 A summary of the risk profile setting out the most significant risks faced by the Unit to be prepared. For each risk, the report shall

a. describe the risk under appropriate category with the assigned risk score;
b. show the key activities and controls to mitigate/manage the risk;

10.4 Further, on a periodic basis, updated information materially affecting the Unit's/Plant's risk profile shall be provided by the Unit/Plant CXOs which would enable the Board to understand the likely future risk profile of VARROC. These shall be reported to the RM Committee and to the Audit committee, if required by the CRO as soon as practicable.

10.5 The Chief Internal Auditor, as part of the internal audit of various Units and corporate functions, shall perform risk-based Audit. The Audit shall include, inter alia, checking on the mitigation measures being undertaken by the Business Units/Plants and verification of the risk rating scores being applied. The Audit Committee shall review these reports of the Chief Internal Auditor.

11. REVIEW AND AMENDMENT

The policy has been approved by the RM Committee and Board of Directors of the Company. The RM Committee and Board may, as and when it deems appropriate, review this policy.

This policy is being formulated keeping in mind the applicable laws, rules, regulations, and standards in India. If there is an amendment in such laws, rules, regulations, governing Act(s) and standards, impacting the provisions of this policy then this Policy shall be deemed to have been automatically amended / modified to the extent of such amendment, even if not incorporated in this policy.

Conversely, if due to subsequent amendment in the statutory provisions, this Policy or any part hereof becomes inconsistent, such amended statutory provisions shall prevail and this Policy shall be deemed to be amended to that extent.

The policy will be reviewed as and when required but at least once in two years. The Board has the power and authority to amend and modify this Policy considering modifications and amendments in SEBI Listing Regulations and Act or otherwise.

Reviewed & amended on February 7, 2023.

---End of document---