Risk Management Policy

Release Date	December 11, 2014
Revision Date	June 24, 2021
Issued by	Risk Management Committee
Supersedes	Released dtd. March 17, 2020

Table of Contents

1.1 INTRODUCTION:

Risk is an inherent aspect of the dynamic business environment. Risk is the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action. Risk arises on account of uncertainty of occurrence and unknown consequences if the risk event were to occur. The degree of uncertainty or likelihood of occurrence and impact of the risk outcome combined together determine the magnitude of the risk.

1.2 PURPOSE OF THE POLICY:

To have a documented Risk Management Strategy in place, which provides a framework for identification, assessment, evaluation, mitigation and review of the risk categories on a periodic basis.

This policy document also lays down the framework for taking informed business decisions integrated with risks and to minimise the adverse consequences of risks on business objectives.

THE RISK MANAGEMENT POLICY:

2. DEFINITIONS:

Inherent Risk: The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls).

Risk Mitigation: Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

Residual Risk: Upon implementation of mitigation actions there will still be a degree of residual (or remaining) risk, with the expectation that an unacceptable level of residual risk would remain only in exceptional circumstances.

Risk Appetite: Risk Appetite is the amount of risk, on a broad level, an organisation is willing to accept in pursuit of value.

3. BLUE STAR'S RISK MANAGEMENT ORGANISATION STRUCTURE

Responsible Person/Team	Constitution	Roles and Responsibilities	Accountable To
Risk Management Committee	Comprises 4 members: - 2 Executive Directors (1 Executive Directors as Chairman of RMC), - 1 Independent Directors - Group CFO	*To frame, implement and monitor the Risk Management Plan for the Company *To ensure that the Risk Management Policy is being followed *To ensure that appropriate measures are taken to achieve prudent balance between risk and rewards in both on-going and new businesses *Assist Board in effective operation of the risk management systems by performing specialized analyses and quality reviews *To ensure that the Company has a robust compliance framework and review the compliance reports and ensure appropriate measures for compliance adherence *Maintain an aggregated view on the risk profile and the underlying business segments *Report to the Board, details on the risk exposures and actions taken to manage the exposures *Advise the Board with regard to risk management decisions, in relation to the strategic and operational matters such as corporate strategy, mergers and acquisitions and related matters *Make regular reports to the Audit Committee and Board on risk assessment and mitigation strategies adopted by the Board *Annual review of key risks which will be monitored closely by the risk committee *Annual review of the Black Swan risk of the Company *Half-yearly review of the Business Portfolio matrix * Periodic review of Business Continuity plan and policy	Board of Directors
Primary Risk Owners	Business/ Functional Heads of each Risk Management Units	*Identify and propose risks, evaluate the criticality and formulate steps for mitigation *Review progress on mitigation action plan and its effectiveness on a quarterly basis *Monitor the movement of KRI and endeavour to maintain the same within the risk appetite	Risk Management Committee (RMC)
Commercial Heads	All India Commercial Head / Department Heads	*Support the Primary Risk Owner in evaluating the risk *Monitor the mitigation action plans *Update risk registers with additions/deletions of risk mitigation actions as approved by the Risk Management Committee	Primary Risk Owners

Responsible Person/Team	Constitution	Roles and Responsibilities	Accountable To
Risk Champion	Nominated by Commercial Head	*Update KRI and the data points to track status of mitigation actions on a quarterly basis	Commercial Head
Central Risk team	Team Leader : A leader from the Finance Team (nominated by the Group CFO) & Risk and Control Management Team	*Support to Commercial Heads in adhering to this policy and the Risk Management framework *Co-ordinate and schedule Risk Committee and Risk Review meetings *Independently test the effectiveness of risk mitigation actions *Draft risk analysis, risk treatment and control mechanism *Perform industry benchmarking and implement best practices *Track actions proposed in the Risk Committee meeting and risk review meetings *Ensures that the risks that may impede achievements of long term strategic plans and their risk mitigation plans are included in the Risk Register.	Group CFO

4. BLUE STAR'S RISK MANAGEMENT FRAMEWORK

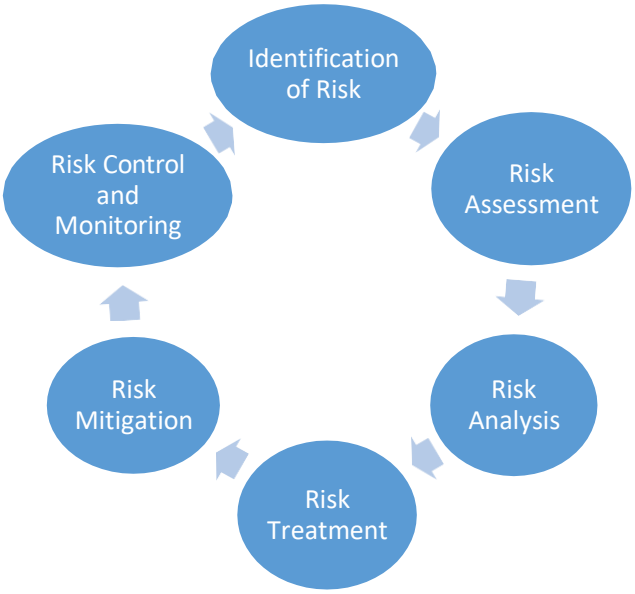
The Company has adopted the Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2017 framework for its Enterprise Risk Management processes.

The Company's risk management framework sets the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management capability. Undertaking a periodic review to assess the effectiveness of the Company's risk management framework is necessary to ensure that the framework continues to evolve and meet the needs of the entity.

Integration of the Risk Management Framework with business objectives and monitoring effectiveness of the mitigation measures through a review of Key Risk Indicators ensures effectiveness of the Risk Management Framework.

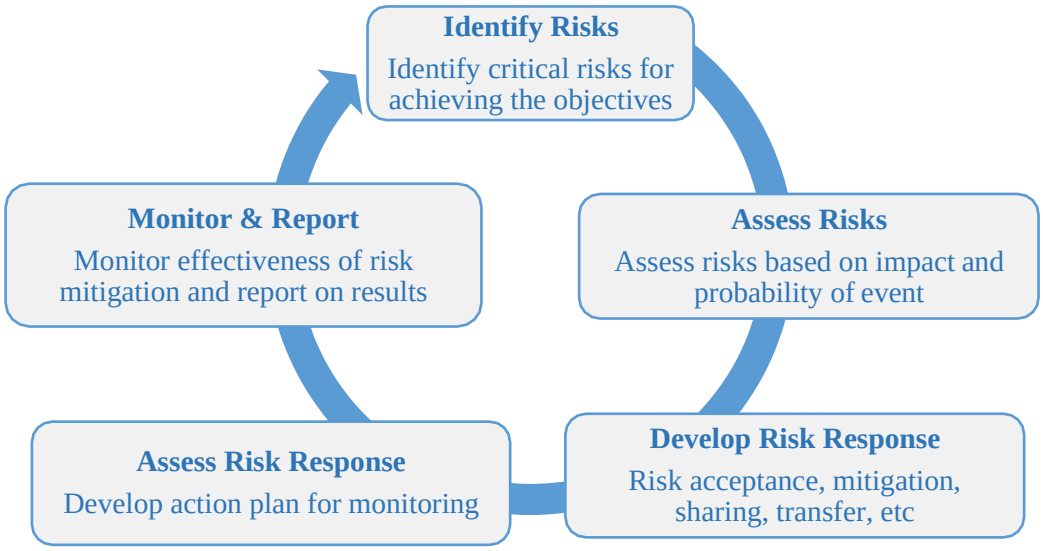
5. THE RISK MANAGEMENT PROCESS:

Risk Management is a continuous process that is accomplished throughout the life cycle of the organisation. Effective Risk Management covers risk management planning, early identification and analyses of risks, implementation of corrective actions, continuous monitoring and reassessment, and communication, documentation and coordination.



5.1 Blue Star's 5 Steps of Enterprise Risk Management

Blue Star has adopted Enterprise Risk Management framework prescribed by COSO and established five steps of a robust risk management framework; they are:



5.1.1. Risk Identification

The Company has identified 7 Risk Management Units (RMU), which are aligned with its businesses and support functions. Risk registers for RMU have been validated following a bottoms-up and periodic top down review processes. The framework identifies internal and external risks faced by the Company including financial, operational, sectoral, sustainability (ESG related risks), information and cyber security risks.

Risk identification techniques are elaborated below:

Sources	Description
Internal Audit reports	Internal audit observations are evaluated to identify if any of those could pose a risk and mapped to the risk management framework wherever required
Peer Companies	On an annual basis, risks identified by the company and their mitigation measures are benchmarked with the risks and mitigation measures reported by the peer entities in their Annual Reports to identify blind spots, if any and appropriate action taken to map them into the risk management framework wherever required
Whistle Blower mechanism	Learnings from investigations into whistle blower complaints also help identify process gaps and risks.
Brainstorming	Perceived risks for a business are identified by key members of business teams through a brainstorming discussion every two years which acts as a platform to identify risks and opportunities
SWOT Analysis	During the preparation of the strategic plan the leadership team carries out a SWOT analysis and the weaknesses and threats identified during the said processes serve as inputs for risk identification
Scenario Analysis	Unprecedented or Unexpected events that have the potential to majorly impact the company's operations are evaluated by the Risk Management Committee on an annual basis

The 7 Risk Management Units (RMU) are Electro-Mechanical Projects Group, Air Conditioning and Refrigeration Products Group, Customer Service Group, Blue Star Engineering & Electronics Limited, International Business Group, Water Purification Division and Corporate functions.

Strategic and operating risks of each RMU are captured in their respective risk registers. The risk registers are maintained in an access controlled intranet-based Risk Management Portal.

The RMU head with their respective Commercial Heads and the Central Risk and Control Management team discuss the risks pertaining to the respective RMU once in a year to identify new risks, if any, arising from contemporary developments in the macro-economic environment or the industry to which they belong and update the risk register upon approval by the Risk Management Committee.

The Risk Identification facility (RIF) on the Risk Management Portal is used to highlight emerging risks or add new risks to the risk register on an ongoing basis.

5.1.2 Risk Assessment

Each of the identified risk is assessed for an inherent risk rating on the twin factors of probability/ frequency and impact/ severity and have, accordingly been classified into the following ratings:

a. Very High

b. High

c. Medium, and

d. Low

The process of identifying the likelihood/frequency and impact/severity of risk events is a both quantitative and qualitative process of analysis.

After finalizing the impact and likelihood rating the inherent risk rating is calculated using the formula:

Inherent Risk Rating = Impact X Likelihood
(Refer Annexure 'A' and 'B')

5.1.3. Risk Response

Response to each of the identified risks are assessed in the context of Company's strategic direction and get suitably categorized into one of the following based on their linkage to the key strategic objectives of the Company:

a. Transfer

b. Avoid

c. Accept and absorb impact

d. Manage actively

5.1.4. Risk Mitigation Actions

Detailed mitigation action with timelines along with identified responsibilities for implementation are formulated for risks that are decided to be 'Managed Actively' as a response. Similarly, appropriate policies have been implemented to address the risk categories, mitigation whereof needs to be transferred.

Risks where the response is to either to "Accept and absorb impact" or "Avoid" are addressed as part of the company's strategy development framework in the context of the exposure management appetite that the Company may have for such risks.

5.1.5. Risks Review and Monitoring

The Company has implemented a robust five tiered review and monitoring mechanism structure which provides a firm foundation for the risk governance. The three tiered review mechanism is as follows:

a. Review with the Risk Owners, Commercial Heads and the Group CFO – All the risk registers are reviewed annually in detail along with formulation of revised mitigation plan wherever required.

b. Review by the Executive Directors – Strategic and significant operating risks identified by each of the Risk Management Units are reviewed annually in detail with the Executive Director responsible for the operational oversight on the Risk Management Unit concerned.

c. Review by the Risk Management Committee – The Risk Management Committee identifies every year, certain risks that are strategic from the corporate perspective which if not adequately addressed can have a major impact on the corporate performance. Such risks are reviewed by the Risk Management Committee on a quarterly basis.

d. Review by the Audit Committee – Besides the quarterly meetings, Audit Committee meets once in a year in March to review progress on all governance related matters. As a part of that process, the Audit Committee also reviews the risk registers of all the RMUs.

e. Review by the Board of Directors – Update on mitigation measures against key risks is submitted once in a quarter to the Board of Directors by the Group CFO.

Key benefits from various monitoring and review processes are as follows:

a. Defined accountabilities, responsibilities, authorities and documentation protocol
b. Measurement of actual progress of mitigation action against milestones
c. Providing KRI performance metrics to measure performance of mitigation measures of individual risks
d. Industry benchmarking
e. Identification of new emerging risks
f. Ensure that the risk mitigation measures are effective, efficient and economical

5.1.6. Risk Reporting

All incidents that have a bearing on the effectiveness of the risk mitigation plan are required to be recorded on the Risk Management Portal by the Commercial Heads.

5.1.7. Communication

Regular interaction and engagement with RMU owners and business teams ensures that sufficient awareness and ownership exists towards the identified risk categories under each RMU. Through the year, the central risk management team also organizes training session and workshops for the benefit of all stakeholders.

5.2 Black Swan Events

A black swan event is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Black swan events are characterized by their extreme rarity, their severe impact, and the practice of explaining widespread failure to predict them as simple folly in hindsight.

The Risk Committee along with the Central Risk and Control Management team discuss potential black swan events once in a year and carry out sensitivity analysis to quantify the impact, should any of those events occur. Mitigation actions arising out of that discussion are incorporated in the risk register of the RMU concerned.

6. Annexures

A. Impact and Likelihood Rating

Risk = Impact*Likelihood

Impact

Impact Risk Category	Financial Impact (Impact on Profit / Revenue)	Qualitative Impact
Very High	> 5%	Significant impact on Reputation, Business Capacity, Market Share, Customer relations
High	3% to 5%	Significant but recoverable impact on Reputation, Business Capacity, Market Share, Customer relations
Medium	1% to 3%	Moderate impact on Reputation, Business Capacity, Market Share, Customer relations
Low	< 1%	Relatively insignificant or limited impact on Reputation, Business Capacity, Market Share, Customer relations

Likelihood

Risk Probability	Occurance in the Past	% of Chances	Occurrence in Future
Likely	Similar instances have commonly occured in the past year	Over 80%	Very high, will be almost a routine feature within the immediate next year
Possible	Similar instances have occurred several times in the past year	50% to 80%	High, may arise several times within the next year
Unlikely	There have been 1 or 2 similar instances in the past year	5% to 49%	Possible, may arise one or twice with in the immediate next year
Remote	Similar instances have never occurred	less than 5%	Not likely, almost impossible to occur between 2 (from now) to 5 years

B. Inherent Risk Rating Heat Map

Risk Impact	**Risk Probability**			
	Low (1)	Medium (2)	High (3)	Very High (4)
Remote (1)	1	2	3	4
Unlikely (2)	2	4	6	8
Possible (3)	3	6	9	12
Likely (4)	4	8	12	16

	Very High risk (12-16)		High risk (8-9)		Medium risk (3-6)		Low risk (1-2)

C. Mitigation Plan Effectiveness Assessment

Mitigation Effectiveness is the effectiveness/existence of controls with respect to the assessed risk in the existing business processes. Mitigation effectiveness is measured on a 3 level rating scale:

	Needs Improvement	Mitigation Plans though in place but do not ensure any control over risk occurrence and impact
	Reasonably Adequate	Mitigation Plans involved duly laid down approval and reporting norms though not ensuring complete control over the risk occurrence and impact
	Effective	Mitigation plans involved stringent approval and reporting norms with responsibility for execution duly mapped to various management levels ensuring complete control over the risk occurrence

D. Residual Risk Rating

(After considering effect of Mitigation Plans)

Mitigation Effectiveness	**Residual Risk Effectiveness Rating Matrix**			
	Inherent Risk Rating			
	Low (Green)	Medium (Yellow)	High (Orange)	Very High (Red)
Needs Improvement	Low (Green)	Medium (Yellow)	High (Orange)	Very High (Red)
Reasonably Adequate	Low (Green)	Low (Green)	Medium (Yellow)	High (Orange)
Effective	Low (Green)	Low (Green)	Low (Green)	Medium (Yellow)