HOOGHLY COCHIN SHIPYARD LIMITED

Risk Management Policy Document

Version 1.0: August 2022

Table of Contents

CHAPTER 1

1.1 Introduction

Risk Management is inherent in any enterprise. Each enterprise has to combat risks which are external to its environment as well as those which results from its business activities. The success of each enterprise depends to a large extent on how effectively it can identify opportunities and risks and how proactively it is able to deal with them. An effective risk management therefore helps a business enterprise to grow and achieve success in all its business endeavors

Hooghly Cochin Shipyard Limited (HCSL) has identified a need for an efficient and effective risk management process and for adoption of a self-regulatory processes and procedures for ensuring that the business is conducted in a risk conscious manner.

The purpose of the Risk Management policy is to put in place a comprehensive risk management system consisting of a defined process of risk management and methodology for identification, assessment, response, monitoring and reporting of risks. The Risk Management Policy would provide the Management and the Board of Directors an assurance that key risks are being properly identified and effectively managed.

Risk Management System and Structure

The board at the helm will review the risk management system within the organization. The board shall discharge its responsibility of risk oversight by ensuring the review at periodical intervals. The board may also delegate to any other person or committee the task of independently assessing and evaluating the effectiveness of the risk management system.

The HCSL management comprising of HCSL Board Level and Below Board level executives will be entrusted with the implementation of the risk management process.

1.2 Risk Management Vision Statement

Minimize the organizational risks to an acceptable level and adopt risk management practices which would help the company to attain its goals and objectives while at the same time ensuring minimization of risks.

1.3 Risk Management Policy

1. The Risk Management process is implemented to improve the company's ability to prevent risks or timely detection of risk and corrective actions
2. To identify risks and mitigation measures
3. Standardization of Risk Management process
4. Facilitate sharing of risk information

The risk management policy intends to put in place an effective risk management framework and an appropriate reporting mechanism. The management of Hooghly Cochin Shipyard would periodically analyze the impact of external and internal

environment and its changes vis a vis the policy framework. The board may approve changes to the policy from time to time in order to align it with the changes in business environment. The policy complements and does not replace other existing compliance programs. The policy is framed based on principles of sound risk management.

1.4 Applicability

This policy is applicable from the date of approval of the Board and applies to whole of the company and includes all functions, departments, business units.

1.5 Risk Management Objectives

The objective of Risk Management is to help management make informed decisions which will:

- Provide a sound basis for good corporate governance;
- Avoid major surprises related to the overall risk and control environment
- Protect & enhance stakeholders' value
- Promote an innovative, risk aware culture in pursuit of opportunities to benefit the company
- Promote qualitative and consultative risk taking

1.6 The Guiding Principles

Risk Management is not a onetime event or exercise; rather it is a process which encompasses series of continuous actions that permeate into the activities of the company. Risk management is not an end in itself but rather an important means to develop organizational resilience. The risk management principles applicable to the company are as elaborated below:

- All risk management activity will be aligned to corporate aims, objectives and organizational priorities set by the company
- Risk management in the company shall be proactive and reasoned (dynamic, iterative and responsive to change)
- Risk management shall be systematic & structured to address uncertainty and shall be an integral part of decision making
- Managers and staff at all levels, directly or indirectly, will have a responsibility to identify, evaluate and manage and / or report risks

1.7 Definitions

This Risk Management policy is formed around a common understanding of terminology used in this document.

Risk

Risk is the potential for loss or harm – or the diminished opportunity for gain – that can adversely affect the achievement of an organization's objectives.

Risk may be a direct or indirect effect on an organization resulting from inadequate or failed internal processes, people & systems or from external events.

Gross Risk
Gross / Inherent risk refers to impact of a risk considering that the risk responses / controls are either absent or ineffective

Residual Risk
Residual risk refers to risk remaining after considering existing controls / implementation of a risk mitigation plan.

Risk Management
The systematic process of identifying, analyzing, and responding to risk events that have the potential to generate adverse effect on the achievement of organizational objectives.

Risk Appetite
Risk appetite is defined as the amount of risk on a broad level an organization is willing to accept in pursuit of value.

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. An illustrative list of risk category along with their definitions is attached as **Annexure I**. This list may be modified in future to add / modify new risk categories that may emerge.

Risk Statement
Risk statement is the description of the risk event(s) along with the likely effect/ impact on the organizational objectives

Contributing Factors
Contributing factors are the possible proximate causes which jointly or severally accentuate the chances of the occurrence of a risk event or increase the level of impact of the risk on the organization.

Risk Analysis
The process of determining the possibility of occurrence of the risk event (Likelihood) and the magnitude of their consequences (Impact) on the organization.

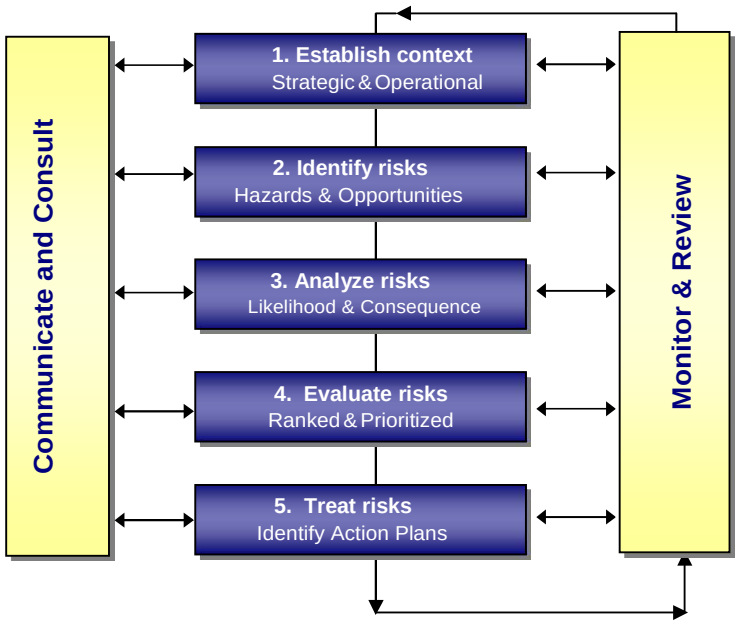
Risk Evaluation
The process used to determine risk management priorities by comparing the level of risk against predetermined standards to generate a prioritized list of risk for further monitoring and mitigation.

Risk Assessment
Risk assessment is the combined process of risk analysis and risk evaluation.

CHAPTER 2

2.1 Components of Risk Management

The various aspects of the Risk Management Process can be represented as below:



A. Communicate and Consult

To communicate and deliberate with various stakeholders both internal and external at every stage of the risk management process.

B. Monitoring and Review

Every stage of the risk management process is to be monitored for effectiveness and improvement.

1. Context

The process will define the circumstances and contexts vis a vis the risk management process. The criteria for evaluation of risk to be established and the structure of the analysis to be defined.

2. Identify risks

To identify and define the events which could affect the achievement of the company's objectives.

3. Analyze risks

To identify and evaluate the existing controls and define the likelihood of risks. This would determine the level of risk. This exercise will also consider the range of potential consequences of the risks and how these could occur.

4. **Evaluate risks**
   Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required and about priorities.

5. **Treat risks**
   Develop and implement specific cost-effective strategies and action plans for increasing potential benefits and reducing potential costs.

2.2 Governance Structure

The Risk Management Structure, roles and responsibilities are set out in Chapter 3.

2.3 Risk Management Approach

The Risk Management Approach is explained in detail in Chapter 4.

2.4 Role of Internal Audit Function

The company recognizes the synergy and inter-dependence between the internal audit function and the risk management program and wishes to draw up a plan that will ensure that:

- Internal audit plans are drawn up based on outcomes of risk assessment program;
- Internal audit function provides effective, independent and objective evaluation of risk management process at regular intervals;
- Risk management program receives constant inputs on controls evaluation from the internal audit function;

2.5 Documentation

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

The documentation will serve the following purposes:

- provide evidence of a systematic approach to risk identification and analysis;
- provide a record of risks to support the development of a database of the company's risks;
- provide risk mitigation plans for approval and subsequent implementation;
- provide accountability for managing the risks identified;
- facilitate continuous monitoring and review;
- provide an audit trail; and
- share and communicate risk management information across the company.

The responsibility for documenting individual risks specific to business functions would be assigned to the functional Risk Management Committee. The designated Chief Risk Officer ('CRO') would be responsible for ensuring that the required documentation required at the corporate level has been developed and maintained up to date. The Risk Coordinators ('RC') at the function level would be responsible for ensuring that the required documentation required at the function level has been developed and maintained up to date.

The key documents pertaining to the risk management process that need to be maintained by the company are:

- **Risk Management Policy**
  The policy provides the overall framework for risk management process of the company. Further amendments will be initiated by the Risk Management Steering Committee ('RMSC') and approved by the Board.

- **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 (Enterprise Risk Register) is owned by the RMSC and will be maintained by the CRO. The functional level risk registers will be owned by the respective Risk Management Committee ('RMC') and will be maintained by the Risk Coordinators at unit level. A template of the risk register is given at **Annexure III**.

- **Risk Management Meeting Template:**
  The RMSC/ RMC meeting template is used to document the minutes of RMSC and RMC meetings. The template aids in capturing and documenting the key discussion points and decisions taken during the meetings. A template for RMSC/ RMC meetings is given as **Annexure IV**.

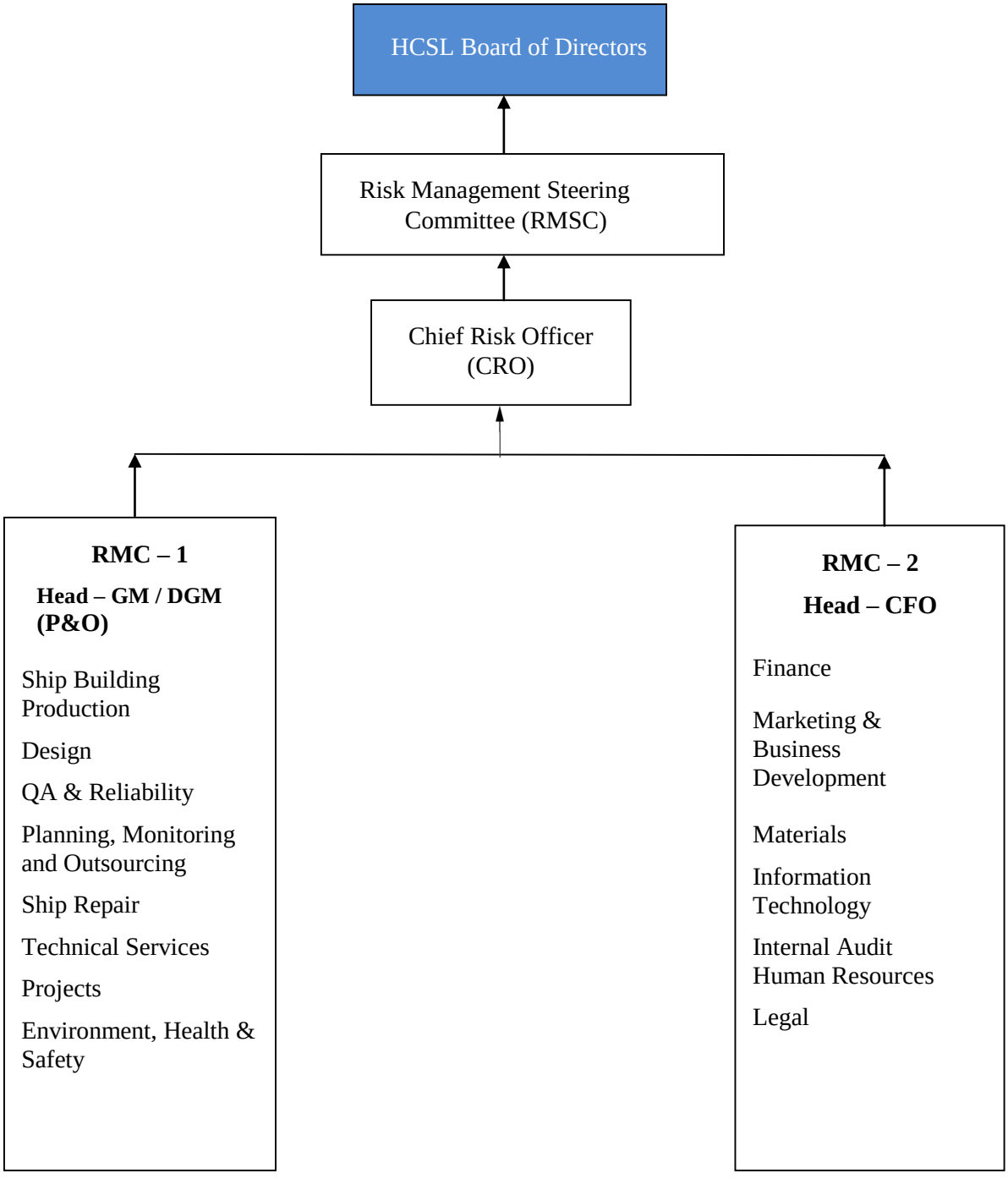
- **Risk Profile:**
  Risk profile helps the management and Board to effectively monitor the management of the risk faced by the company. It provides detailed description of the risk and related information required for proposing and documenting mitigation plan to reduce the risk exposure. A template for profiling is given at **Annexure V**.

[Space left blank intentionally]

CHAPTER 3

3.1 HCSL Risk Management Governance Structure

The following diagram gives an overview of the risk management governance structure to be implemented in HCSL



3.2 Risk Management Steering Committee ('RMSC')

The RMSC is the apex committee in the RM governance structure comprising of key decision makers within the organization. RMSC is entrusted with the responsibility of implementing the risk management framework across the organization. RMSC will apprise Board of Directors about various risk management initiatives and ensure adequate reporting of the same to various stake holders on a regular basis.

Constitution

The RMSC shall consist of the CEO, CFO and the Head GM/DGM (P&O). CEO shall be the Chairman of the Committee.

Operation and periodicity of meeting

The RMSC shall meet on half yearly basis or more frequently if required for urgent matters. The Chief Risk Officer ('CRO') will act as the convener for the meetings of RMSC and will be responsible for maintaining the reports of RMSC's activities (agendas, decisions) and minutes of meetings (including attendance).

Roles and Responsibility

The roles and responsibilities of RMSC shall be as given below:

(i) Monitoring and reviewing of the risk management plans including steps taken for ensuring cyber security;

(ii) Ensure required risk documentation is done on quarterly basis;

(iii) Provide updates and seek approval from Board of Directors on risk management;

(iv) Initiating amendments to the Risk Management Policy, wherever found appropriate and obtaining approval of the Board; and

(v) Such other functions as may be specified by the Board from time to time.

3.3 Risk Management Committees ('RMC')

The RMC is the committee, formed at the functional level, in the risk management governance structure comprising of key decision makers within the respective function/unit. It is responsible for adopting and implementing the risk management framework at their respective function/unit.

Membership

The composition of various RMC's within HCSL is as given in **Annexure II**.

Operation and periodicity of meetings

The designated Risk Coordinator will coordinate activities relating to the RMC. The RMCs

shall meet on a quarterly basis or more frequently if required for urgent matters. Reports of RMC's activities (agendas, decisions) and minutes of meetings (including attendance) will be maintained for each meeting by the Risk Coordinator of the individual RMCs.

The functional heads and other senior personnel may be invited to participate in the committee meetings as required.

Roles and Responsibilities

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

- Quarterly and need basis review of function wise risk registers including identification of new risks
- Review risk profile document on risk mitigation plan and its implementation status
- Provide updates and seek approval from RMSC on risk management

3.4 Chief Risk Officer ('CRO')

The CRO will be appointed by the Risk Management Steering Committee (RMSC) and the CRO would be permanent invitee to RMSC. The CRO shall be the coordinator for risk management activity for the entire company. The CRO shall liaise with the Risk Coordinators (RCs) to coordinate flow of information between them and the RMSC. The CRO shall be responsible to ensure supply of information for the meetings of the RMSC held half yearly or as required, to review the risks identified. The CRO will act as the convener for the meetings of RMSC and will be responsible for maintaining the reports of RMSC's activities (agendas, decisions) and minutes of meetings (including attendance). The CRO shall be responsible to apprise the RMSC and Board of Directors about the status of the Enterprise Risk Management (ERM) at the company.

3.5 Risk Owners and Risk Coordinator

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 existing controls and thereby propose risk mitigation plans for the assigned risk. Risk Owner is also responsible to implement the approved mitigation plan and periodically review the implementation status of mitigation plans.

The Risk Coordinators would be a member of the respective RMC's and be responsible as coordinator for risk management activities for their respective functions. The Risk Coordinator would liaise with the Risk Owners to coordinate flow of information between them and the RMC. The Risk Coordinators would be responsible to ensure that meetings of the RMC are held quarterly or more frequently as required to review the risks identified, and necessary attendance and minutes of meetings are maintained. The Risk Coordinator would be responsible to apprise the RMC Head and the CRO about the status of the risk management at their respective RMC. The Proof of risk mitigation measures implemented by the concerned Risk Owner to be submitted on a quarterly basis by the Risk Coordinator to the functional Risk Management Committee and CRO.

Risk Owners and Risk Coordinator will be nominated by the respective RMC Head.

3.6 Roles & Responsibilities

The risk management roles and responsibilities will be as follows:

Roles	Responsibilities
Board of Directors	• Approve risk management policy • Review risk management process and provide inputs/ directions, if any, to the executive management • Set 'Risk Appetite' for the company
Risk Management Steering Committee (RMSC)	• Lead the Risk Management initiative within the company • Set standards for risk documentation and monitoring • Recommend training programs for staff with specific risk management responsibilities • Review and approve the risk management report including selection of critical risks to be put before the Board of Directors
Risk Management Committee (RMC)	• Implementing the risk management initiatives across the functions • Review implementation of risk management process including identification and assessment of the relevant risks at functional level • Approve and submit risk documents to CRO/ RMSC • Provide updates to CRO for communication to RMSC on risk management at RMC level
Chief Risk Officer (CRO)	• Review the risk management initiatives across the entire organization and maintain the Enterprise Risk Management (ERM) system • Liaise with the Risk Coordinators to coordinate flow of information and escalation of key risk issues/concerns between the RMSC and Risk Coordinators • Prepare and maintain relevant documentation for ERM for the company and present it to the Board of Directors of the company / RMSC half yearly/ need basis.
Risk Coordinator (RC)	• Liaise with the Risk Owners to coordinate flow of information and escalation of key risk issues/concerns between the RMC and Risk Owners • Ensure that meetings of the RMC are held regularly • Prepare and maintain relevant documentation for the RMC and submit the same to CRO

Risk Owners (RO)	• Ensure preparation of a suitable risk mitigation plan keeping in mind the current controls mechanism in place, proposed mitigation measures and organizational priorities • Ensure that the risk profiles are filled and key risks are escalated to the respective RMC for their approval of proposed mitigation plan • Ensure that the approved plans are implemented within the target timeframe and reported regularly
Employees	• Assist in complying with risk management policy adopted by the company • Responsible for identifying risks and escalating risks to the next level • Exercise reasonable care to prevent loss, to maximize opportunity and to ensure that the operations, reputation and assets are not adversely affected

3.7 Summary of Periodic Activities by Role:

A summary chart displaying the activities to be followed periodically is given below:

Roles	**Periodicity of Meeting**	**Activities**		
		Quarterly and need basis	*Half-Yearly and need basis*	*Yearly and need basis*
Risk Owner	-	• Review and update Risk Profiles and report to Risk Coordinator	-	-
Risk Coordinator	-	• Update Risk Registers and report to RMC • Present updated Risk Registers & Risk Profiles to CRO on behalf of RMC	-	-
Risk Management Committee (RMC)	Quarterly and need basis	• Review of Risk Registers & Risk Profiles • Review Risk mitigation and management status	-	-
Chief Risk Officer (CRO)	-	• Update consolidated Risk Register (Collation of risks submitted by RMCs for escalation) • Present a detailed analysis of critical risks & risk profiles to the RMSC • Present consolidated Risk Register & Risk Profiles to the Board half yearly and on need basis	• Present top risks areas as identified by RMSC to the Board	• ERM implementation status report to the Board

Risk Management Steering Committee (RMSC)	Half-Yearly and need basis	• Review of consolidated Risk Register & Risk Profiles	-	• Review of Risk Appetite Statement
Board of Directors	Half-Yearly and need basis	-	• Review of top risk areas	• Review the progress of ERM implementation • Approval of Risk Appetite Statement

CHAPTER 4

4.1 HCSL Risk Management Process

Organizations encounter risk every day as they pursue their objectives. In conducting appropriate oversight, management and the board of the company are responsible for describing, how much risk is acceptable in pursuing these objectives. To fully embed ERM in HCSL, decision makers must know how much risk is acceptable as they consider ways of accomplishing objectives, both for their organization and for their individual operations (division, department, etc.)

4.2 Approach

Defining a risk appetite statement starts with analyzing the long-term and short-term goals of the company. The company should be able to identify its strategic and tactical objectives.

Based on the strategic and tactical objectives a broad statement depicting the overall risk appetite of the organization shall be defined. In addition, risk tolerance levels for the following broad organizational objectives shall also be defined:

- Strategic - high-level goals, aligned with and supporting its mission
- Operational - effective and efficient use of its resources
- Reporting - reliability of reporting
- Compliance - compliance with applicable laws and regulations

HCSL's risk appetite and risk tolerance is given in section 4.3 below

4.3 Responsibility

The Board shall be responsible for defining the risk appetite statement for the company.

The Risk Management Steering Committee shall be responsible for reviewing the risk appetite of the company on a yearly basis and revising the same based on changes in internal/ external business environment and stakeholder expectations. Any changes made to the risk appetite needs to be approved by the Board.

4.4 HCSL's Risk Appetite Statement

The prevailing risk appetite statement for the company is defined as follows:

The Organization operates within a low overall risk range. The Organization's lowest risk appetite relates to operational, compliance and reporting objectives, with a marginally higher risk appetite towards its strategic objectives.
This means that reducing to reasonably practicable levels the risks related to product defects, delivery and productivity. Meeting legal & compliance obligations will take priority over other business objectives.

HCSL Risk Appetite

STRATEGIC	OPERATIONAL	REPORTING	COMPLIANCE
High risk tolerance for: • Delays in project implementation (modernization and expansion) • Potential failure in pursuing research for new design and related technology • Higher losses in the pursuit of diversification and expansion of existing business • Potential failures in efforts for enhancing brand value	**Low risk tolerance for:** • Product defect and quality issues • Delayed deliveries • Underutilization of capacities (facilities and human resources) • Employee health and safety	**Low risk tolerance:** • Concerning the possibility of significant or material deficiencies in internal controls • Concerning the quality, timing, and accessibility of data needed to run the business. • Related to financial reporting quality (timeliness, transparency, GAAP, etc.)	**Very low tolerance for:** • Violations of legal and regulatory requirements including code of ethics / fraud prevention policy of the company'

4.5 Risk Management Process Steps

4.5.1 Risk Identification

Risk Identification is a process of identifying risks for assessment, evaluation and determination of appropriate mitigation plans. A systematic process of comprehensive risk identification is the foundation on which edifice of risk management is built.

The company may use following tools & methodologies to identify new risks that may have emerged or risks that would have changed over a period of time:

- Structured workshops;
- Brainstorming sessions;
- Interviews by CRO and / or the Risk coordinators;
- Review of loss event;
- Review of documents.

All identified risks shall be updated in a risk register. Risk registers shall be quarterly reviewed and updated by the respective Risk Management Committees to ensure pertinence of the risks listed.
Risks that would have ceased shall also be closed appropriately. The CRO and Risk Coordinators shall ensure that the risk registers are reviewed and updated quarterly.

4.5.2 Risk Assessment

The risks shall be assessed on qualitative two-fold criteria. The two components of risk

assessment are:

a) The likelihood of occurrence of the risk event, and
b) The magnitude of impact if the risk event occurs.

The risks shall be assessed according to the risk assessment criteria defined in **Annexure VI** The combination of likelihood of occurrence and the magnitude of impact provides the risk level. The magnitude of impact of an event (if it occurs), 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:

Table for Likelihood levels

Levels	Descriptors
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:

Table for Impact levels

Levels	Descriptors
5	Very High impact
4	High impact
3	Moderate impact
2	Low impact
1	Very low impact

4.5.3 Risk Evaluation

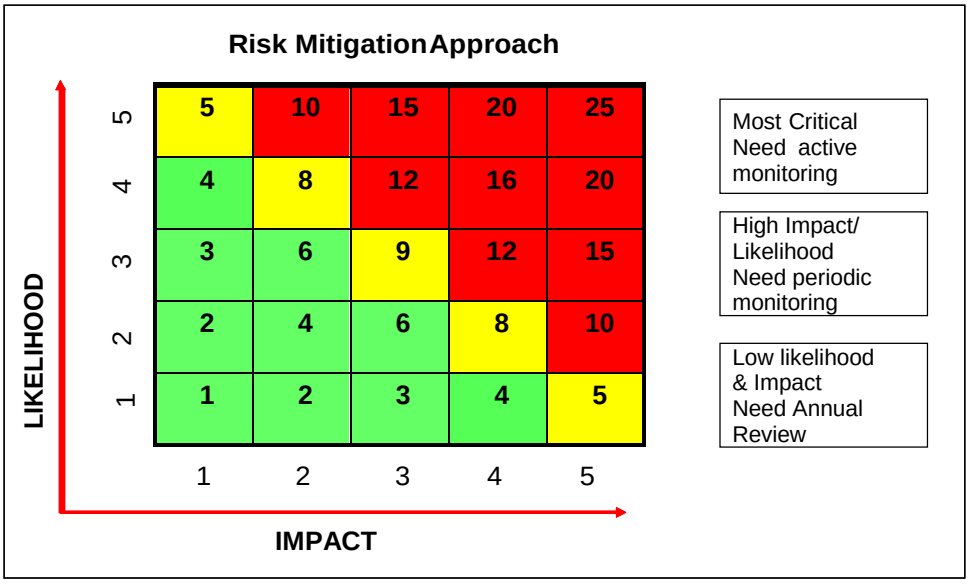
For each risk, the average score for likelihood and impact shall be multiplied to arrive at a combined score. In case the rating of risks is done by a group, average of the group's score shall be determined. The average is to be determined for each component of risk assessment viz., Likelihood and Impact. The simple average for each component of each risk shall be calculated.

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 (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 mitigation 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 evaluation is to assist the organization in prioritizing risk to ensure that appropriate attention is given to risks based on their criticality and that company resources are effectively utilized in managing these risks.

4.5.4 Risk Mitigation Plan

The risk mitigation plan adopted by the company would also depend on the vulnerability factor. Vulnerability is the extent to which the organization may be exposed in relation to various risk factors after existing controls have been taken into consideration. Vulnerability differs from the likelihood as likelihood only considers the probability of an event occurring whereas vulnerability also considers other aspects such as control effectiveness and level of preparedness to deal with risks.

Risk mitigation involves identifying the range of options for mitigating risk, assessing those options, preparing risk mitigation plans and implementing them. Mitigation 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. This option may be taken in cases where the exposure of risk is very high as compared to the expected benefits/ returns in continuing those activities.
- *Acceptance* – No action is taken to mitigate the risk or reduce the likelihood or impact. This option may be taken in cases where the cost of reducing the exposure is very high as compared to the benefit accrued from reducing the risk exposure.
- *Reduction* – Developing mitigation plan to reduce risk exposure. Mitigation plans need to be developed and implemented for reducing the risk exposure.
- *Transferring* – Includes purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.

Mitigation plan for each risk shall be documented in the risk profile template provided in **Annexure V**. The profile contains details of the risk, its contributing factors, risk scores, controls documentation, and specific and practical mitigation plans. Mitigation plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining procedures and processes in place and additional resource allocation that will ensure that existing level of risks is brought down to an acceptable level. In many cases significant risk may still exist after mitigation of the risk level through the risk mitigation process. For risks considered to be "acceptable" risk profile will be developed with mitigation plan as accepted and no further actions required.

4.5.5 Escalation of risks

It is critical to institute an effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately. Every employee of the company has responsibility of identifying and escalating the risks to appropriate levels within the company. A template for proposing new risks is prescribed in **Annexure VII**.

After the risk is identified upward escalation of the same will be as below:

1) Risk Management Committee Head to select risks to be escalated which primarily will be of following types:
   a) Critical risks relevant to the function wherein the complete mitigation is possible at RMC level

b) Critical interdependent risks wherein intervention of RMSC/Board is required for smooth implementation of the mitigation plan. It is desired that Risk Owner prepares risk mitigation plan at the unit/function level for such risks which may be considered by RMSC/Board for integrated response/mitigation plan

2) The CRO shall select high value risks to be escalated to RMSC based on the inputs received from respective RMCs. This would include:

i) Risk submitted by individual RMCs as critical for their respective function

ii) For critical interrelated risks the CRO need to present to the RMSC, an aggregate/consolidated view of the risks after thorough analysis and consultation with RMC heads of relevant Business Unit/ Corporate Function

iii) RMSC will review the risks submitted by CRO and will identify and escalate strategic risks to the Board

4.5.6 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 mitigation options.

Risk review aims at assessing the progress of risk mitigation plans. It also ensures that the current assessments remain valid. The risk register shall be reviewed, assessed and updated on a half yearly basis by the RMSC.

The Risk Owners shall periodically review the risks owned by them to ensure that ratings remain pertinent and to monitor the status of mitigation plans. The CRO shall periodically review the risk register, risk profiles and status of mitigation plans.

4.5.7 Closure of risks

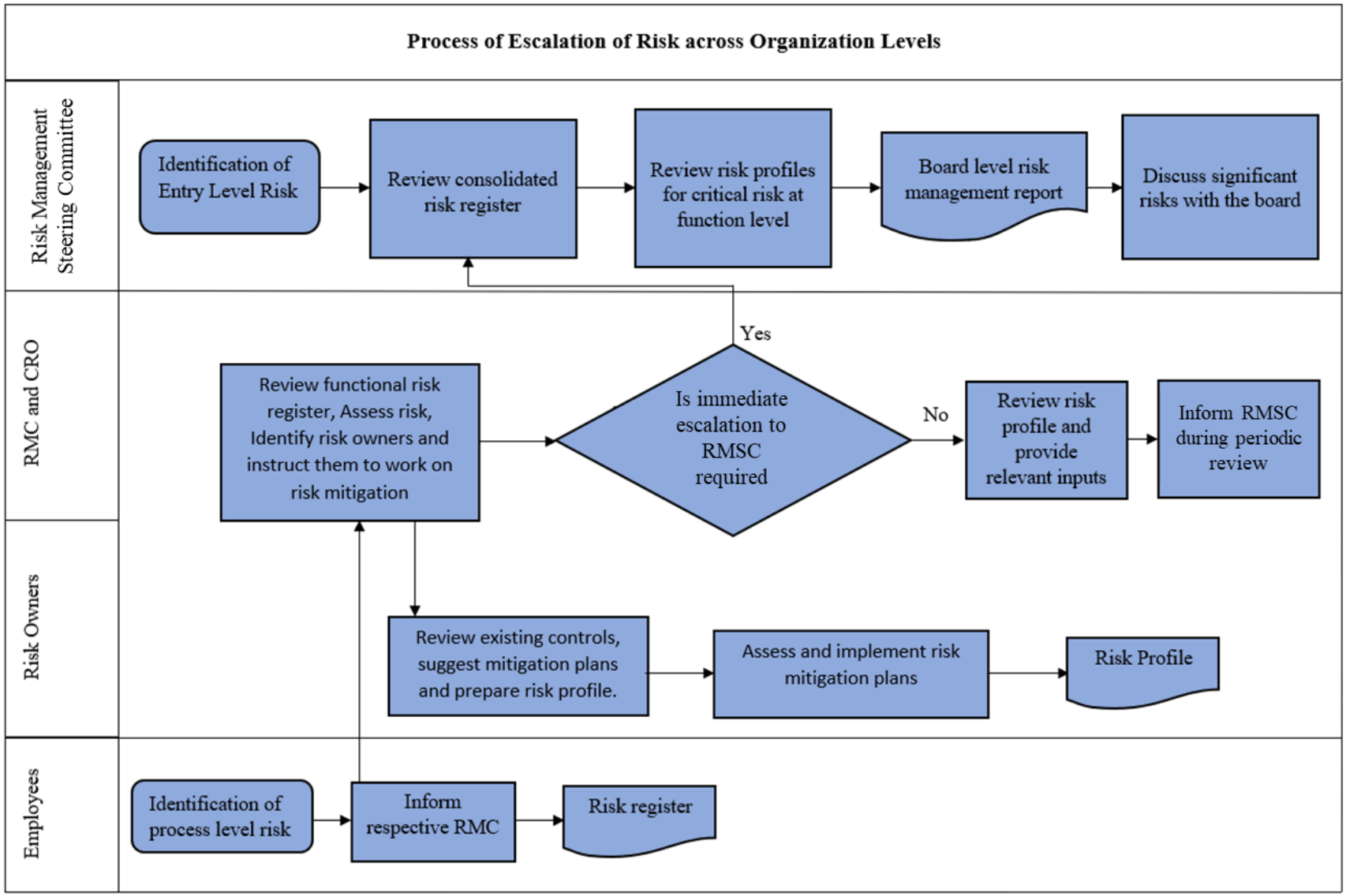
A risk issue identified and documented shall not be deleted from risk registers and shall be closed after the approval of respective RMC, due to any one of the following reasons:

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

4.5.8 Reporting

A report comprising of top critical risk areas (including mitigation plans) duly approved by the RMSC, shall be placed before the Board. On an annual basis, the Board would review the progress of risk management implementation (including areas such as training requirements, process improvisation etc.).

****


Process of Escalation of Risk across Organization Levels
Risk Management Steering Committee
RMC and CRO
Risk Owners
Employees
Identification of Entry Level Risk
Review consolidated risk register
Review risk profiles for critical risk at function level
Board level risk management report
Discuss significant risks with the board
Yes
Review functional risk register, Assess risk, Identify risk owners and instruct them to work on risk mitigation
Is immediate escalation to RMSC required
No
Review risk profile and provide relevant inputs
Inform RMSC during periodic review
Review existing controls, suggest mitigation plans and prepare risk profile.
Assess and implement risk mitigation plans
Risk Profile
Identification of process level risk
Inform respective RMC
Risk register

Annexure I: Illustrative list of risk categories

Sr. No.	Risk Classes / Baskets	Definitions
1.	Strategy	Risks associated with strategy development, strategic alliances, business planning, business model, growth, reputation, innovation and performance targets.
2.	Marketing and Sales	Risks associated with developing, implementing, and managing new and existing products, customer service, pricing, marketing and feasibility of new business opportunities.
3.	Capital Projects	Risk associated with planning, organizing and managing resources to bring about successful completion of capital expenditure objectives.
4.	Operations/ Production	Risks associated with production planning, production scheduling, environmental & operational safety, inventory management and quality control. Also includes risks associated with inadequate or failed internal processes, people and systems, or from failure of infrastructure largely having to do with the performance, protection and utilization of existing assets.
5.	Human Resource (HR)	Risks associated with culture, organizational structure, communication, recruitment, performance management, remuneration, learning & development, retention, OH&S and industrial relations, including supporting systems, processes, and procedures.
6.	Corporate Planning	Risk associated with a lack of defined policies, processes, procedures or delegations of authority at a group, business unit or product area.
7.	Budgeting/ Forecasting	Risks associated with, budgeting, management reporting and cost management.
8.	Information Technology (IT)	IT risk include issues like IT strategy, architecture, infrastructure, networks, support systems, interfaces, data reliability, access controls disaster recovery
9.	Information Security	Risk associated with data loss, fraud, system outages, breach of confidentiality, legal/regulatory violations, as well data integrity.
10.	Finance	Financial risks include risks associated with capital structuring, capital allocation, financial management, debtor's management, forex, hedging and preparation of financial statements.

Sr. No.	Risk Classes / Baskets	Definitions
11.	Contract Management	Risk associated with any partnerships, governmental contracts, concessions, treaties through which an organization conducts business, production-sharing agreements and side-agreements.
12.	Compliance	Risk relating to noncompliance with legislation, regulations, supervision, internal policies and procedures.
13.	Legal & Regulatory	Failure of infrastructure processes, systems, and resources to support legal and regulatory requirements.
14.	Procurement	Risks associated with procurement process, internal and external logistics and transportation, quality controls, outsourcing and vendor relationships
15.	External Factors	The risks associated with external factors like political, economic /markets, social, technological, legal and regulatory, fraud, and environmental conditions pose threat to the organization.
16.	Environment, Health and Safety	This category includes risks related to environment pollution, safety of resources and employees' health, etc.
17.	Reporting	Risk associated with collection of data from internal and external sources and relate to quality and integrity of the data Risk associated with timely and accurate disclosure of data / information like annual reports, MIS to internal and external stakeholders
18.	Business Continuity Planning/ Disaster Recovery	Risk associated with the organization's ability to design, develop, test and implement a strategy to mobilize critical staff during a business interruption, as well as recover infrastructure and data.
19.	Reputation Risk	Reputational risk is a threat or danger to the good name or standing of the business or entity

Note ** This list may be modified in future to add / modify new risk categories that may emerge.

Annexure II: List of Risk Management Committees (RMCs)

For effective implementation of risk management process, the organization has constituted separate Risk Management Committees. The composition of various RMC's within HCSL is as given below:

1. **RMC 1: *Head:* GM / DGM (Operations)**

   Constitutes of:
   - Ship Building Production
   - Design
   - QA & Reliability
   - Planning, Monitoring and Outsourcing
   - Ship Repair
   - Technical Services
   - Projects
   - Environment, Health & Safety

2. **RMC 2: *Head:* CFO**

   Constitutes of :

   - Finance
   - Marketing & Business Development
   - Materials
   - Information Technology
   - Internal Audit
   - Human Resources
   - Legal

Annexure III: Template for Risk Register

Risk ID No.	Risk Category	SBU/Segment	Risk Statement	Likelihood Score	Impact Score	Overall Score	Risk Owner

Annexure IV: Template for Recording Risk Management Meetings

Committee:	**RMSC/ RMC X**
Date & Time:	
Location:	
Participants:	**1. Name (Designation)** **2. Name (Designation)**
Agenda:	
Summary of Discussion:	
Significant Points Discussed:	
Proposed Action Items:	
Name & Signature of RMC coordinator	

Annexure V: Template for Risk Profile

Risk Register Reference No:						
Risk Category:						
Risk Statement:						
Risk Owner:						
Date of Validation:	(dd/mm/yyyy)					
Date of Next Review:	(dd/mm/yyyy)					
Contributing Factors			**Existing Control**			
Ref No.	**Description**		**Description**			**Registered Date**
	• Factor 1 • Factor 2 • Factor n		• Control 1 • Control 2 • Control n			
Type of Risk Rating	**Current Review**		**Last Review**			
A. Likelihood Rating [1-5]:	(Rating score of current review)		(Rating score of last review)			
B. Impact Rating [1-5]:	(Rating score of current review)		(Rating score of last review)			
Overall Risk Rating (A*B):	(Rating score of current review)		(Rating score of last review)			
Risk Type	(Critical/ Cautionary/ Acceptable)					
RISK MITIGATION PLAN						
Sr. No.	**Description**	**Target Date**	**Target Date Decided By**	**Responsibility**	**Submit Date**	**Comments (If any)**
1						
2						
Signatures: _____ **(Risk Owner)** _____ **(Risk Coordinator)** _____ **(Chairman- Risk Management Committee)**						

Annexure VI: Risk Assessment Criteria

The risk assessment criteria for Impact parameter are defined as follows:

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 • Minimal impact on ability to raise finance • No impact on HCSL brand image	• Regional media attention • Loss of reputation for a moderate period of time • Relatively small impact on ability to raise finance • Minor impact on HCSL brand image	• Sustained negative regional media attention • Loss of reputation for a long period of time • Major impact on ability to raise finance • Major impact on HCSL brand image	• Negative national media attention • Loss of reputation for a moderate period of time • Significant impact on ability to raise finance • Significant impact and HCSL brand image	• Sustained negative national media attention • Significant loss of reputation for a long period of time • Critical impact on ability to raise finance • Severely impact the HCSL brand image
Regulatory/ Legal	• Notice of violation /warnings requiring administrative action and minimal penalties	• Local level cases subject to fines or penalties • Subject to administrative action at within local jurisdiction	• Routine state level cases subject to fines or penalties • Subject to regulatory proceedings and/or hearings at state level	Routine central or state cases subject to substantial fines or penalties • Subject to regulatory proceedings and/or hearings	• Major central or state scrutiny, investigations subject to substantial fines and penalties including criminal charges and/or shut down of

				• Noncompliance with MOU	operations • Possible regulatory action • Noncompliance with MOU

The risk assessment criteria for Likelihood parameter are defined as follows:

Criteria	Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Occurrence	• Event may occur in exceptional situations •	• Event may occur sometime	• Event should occur sometime	• Event will occur in most circumstances	• Event is certain to occur in most circumstances
Likelihood/ Probability	• Event could occur once in more than 5 years	• Event likely to occur once in 3 to 5 years	• Event expected to occur once in 3 years	• Event may occur once in a year	• Event certain to occur multiple times in a year

Annexure VII: Template for Proposing New Risks

Employee ID:		**Name**	
Division / Department/ Function		**Designation**	
Mobile No		**Email Id**	
Details of Proposed Risk			
SBU/Segment/Function			
Risk Category			
Risk Statement			
Contributing factor		**Existing Control**	