# DREDGING CORPORATION OF INDIA LIMITED

## Risk Management Policy

Version 2.0: March 2022

CONTROLLED/UNCONTROLLED COPY NO:

REVISION NO: ISSUE DATE:

ISSUED TO CATEGORY: INDIVIDUALS/DESIGNATED RECIPIENT/INTRANET

1. This policy is being issued to:
2. Holder of the controlled copy will receive revisions or additions, as and when issued. Obsolete versions shall be removed by the holder of the controlled copy.
3. When the designated recipient ceases to be in the designated office, he / shall ensure that the controlled copy is passed on to the incoming incumbent.

ISSUED BY:

DATE:

CHIEF RISK OFFICER
(Signature with Seal)

**Table of Contents:**

## Chapter I:Introduction

Significance of risk management is inexorably linked to entrepreneurial activities, and these are inseparably tied up with opportunities and risks. Within the framework of external requirements (such as regulations) and the circumstances specific to each company resulting from its business activity, a company's success is influenced by its recognition of opportunities and risks and the way in which it sets about proactively dealing with them. Effective risk management provides a platform to the organization to grow and thrive successfully in all its business endeavors.

Dredging Corporation of India Limited ('DCI' or 'the Company') has identified a need for an efficient and effective risk management process within the company along with necessary documentation which demonstrates management's acceptance of a set of self-regulatory processes and procedures for ensuring the conduct of the business in a risk conscious manner.

Risk management framework comprising of the Risk Management Policy (the policy) is intended to enable the Company to adopt a defined process for managing its risks on an on-going basis. An important purpose of the policy is to implement a structured and comprehensive risk management system, which establishes a common understanding, language and methodology for identifying, assessing, responding, monitoring and reporting risks and which provides management and the Board of Directors ('the Board') with the assurance that key risks are being properly identified and effectively managed.

The Board shall discharge its responsibility of risk oversight by ensuring the implementation and review of the risk management system within the organization. Board may delegate to any other person or committee the task of independently assessing and evaluating the effectiveness of the risk management system.

This document would be shared with senior and middle management for better understanding and implementation of the risk management process.

## Chapter II:Risk Management Policy

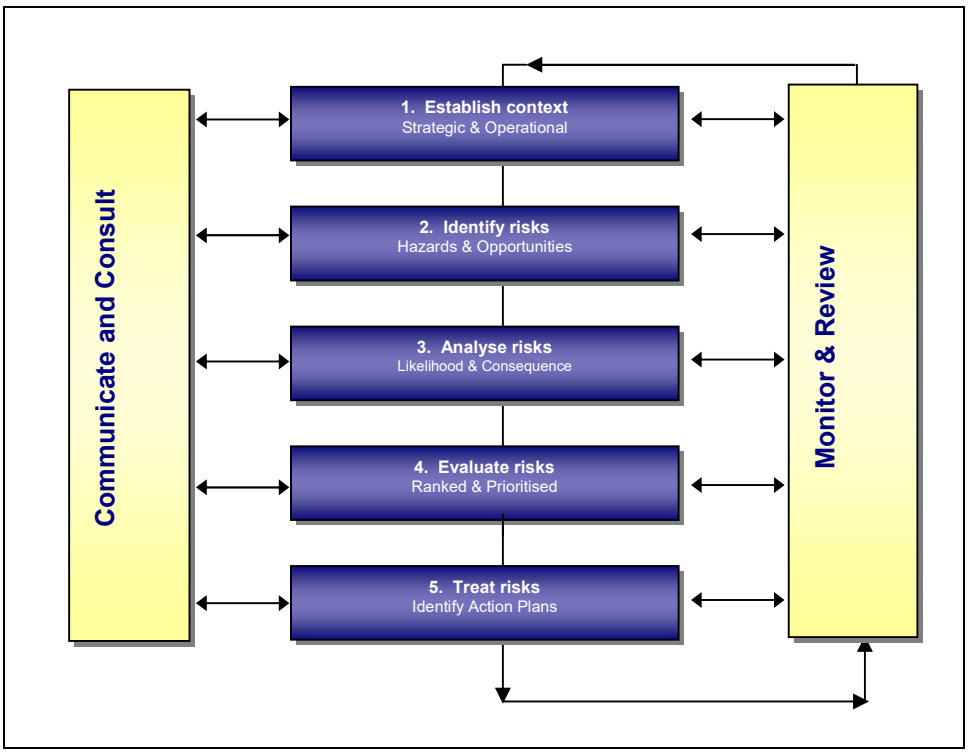
DCI is committed to implement a robust risk management process to:

- improve its ability to prevent or timely detect risk event,
- identify, discuss, escalate and provide suggestions to deal with risk issues;
- standardize risk management principles and language across the company;
- improve sharing of risk information
- provide flexibility for managing upside and downside scenarios

This policy is intended to ensure that an effective risk management framework is established and an appropriate reporting mechanism for the same is embedded within the company.

The management shall periodically assess the impact of changes in external and internal environment on the pertinence of this policy. And if the Board deems fit, it may approve necessary changes to this policy to align it with the prevailing business circumstances.

This policy complements and does not replace other existing compliance programs. This policy is built on the established principles of sound risk management as detailed in recognized sources.



## 2.1 Applicability

This policy is applicable from the date as mentioned on the "Document Control Sheet" and applies to whole of the company and all regions of operations and includes all functions, departments, business units.

## 2.2 Risk Management Objectives

The objective of Risk Management is to help management to take 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

## 2.3 Risk Management 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 DCI. Risk management is not an end in itself but rather an important means to develop organizational resilience. The risk management principles applicable to DCI are as elaborated below:

- All risk management activity will be aligned to DCI aims, objectives and organizational priorities set by DCI
- Risk management in DCI 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

## 2.4 Definitions

This Risk Management charter &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 treatment plan.

**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 Management**

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

**Risk Management Committee (RMC)**

It is the Committee of Directors and officials, constituted by the Board of Directors.

**Risk Coordinators (RC)**

The official/committee of officials nominated by the Head of the Departments. RC is responsible for documenting of risk management processes specific to functional level at respective departments.

**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.

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

## 2.5 Structure

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

## 2.6 Risk Management Structure

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

## 2.7 Key Documents

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

- Risk Management Policy
  Risk Management Policy is robust process to improve ability to prevent or timely detect risk event. This policy focuses on identification, discussion, suggestions and mitigations to deal with risk issues. The policy provides the overall framework for risk management process of the Company. MD & CEO is authorized to make changes as may be required to the Policy.

- 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 will be maintained by the CRO. The functional level risk registers will be owned by the respective Departmental Heads. A template of the risk register is given as **Annexure II**.

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

- 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 as **Annexure IV**.

## Chapter III:Risk Management Governance Structure


### 3.1 Risk Management Committee (RMC)

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

*Membership*
The RMC shall be appointed by the Board complying with the requirements of SEBI (LODR) comprising of
AtleastTwo Directors (including one independent Director)
MD&CEO
Senior Officials of the DCI
Chief Risk Officer
Company Secretary shall be the Secretary of the Committee.

*Operation and periodicity of meeting*
The Chief Risk Officer (CRO) will coordinate activities relating to RMC. The RMC shall meet on a half yearly basis or more frequently if required for urgent matters. The CRO will act as a convenor for the meetings of RMC and Secretary of RMC will be responsible for preparing the reports of RMC's activities (agendas, decisions) and minutes of meetings (including attendance).

*Roles and Responsibility*
The role of the committee shall, inter alia, include the following:
(1) 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, in particular including financial, operational, sectoral, sustainability (particularly Environmental, Social and Governance (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.

(2) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;
(3) To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;
(4) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
(5) To keep the board of directors informed about the nature and content of its discussions, recommendations and actions to be taken;
(6) The appointment, removal and terms of remuneration of the Chief Risk Officer (if any) shall be subject to review by the Risk Management Committee.
(7) The Risk Management Committee shall 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.
(8) Any other items/issues as may be referred to RMC by Board and/or mandated by SEBI or any other statute.

### 3.2 Departmental Risk Management Committee (DRMC)

Every Head of Department at the functional level shall be responsible 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*
All the Heads of Department shall be the Members of DRMC

*Operation and periodicity of meetings*
The DRMCs shall meet periodically (monthly or otherwise with atleast one meeting every two months) or more frequently if required for urgent matters. Reports of DRMC's activities (agendas, decisions) and minutes of meetings (including attendance) to be submitted to CRO through respective Head of Departments.
The functional heads and/or other senior personnel may be invited to participate in the committee meetings as required.

*Roles and Responsibilities:*
The DRMC shall assist RMC in performing the role and responsibilities as assigned to RMC.

### 3.3 Chief Risk Officer (CRO)

The CRO would be a member of the RMC and be responsible as coordinator for risk management activity for the entire company. The CRO would liaise with DRMC to coordinate flow of information between them and the RMC. The CRO would be responsible to ensure that meetings of the RMC and DRMC are held as required, to review the risks identified. The CRO would be responsible to appraise the RMC and Audit Committee/Board of Directors about the status of the risk management of the company. CRO shall report to MD & CEO of Organisation.

### 3.4 Risk Owners

All departmental heads shall be the Risk owners for their respective departments.

### 3.5 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 responsibility for documenting individual risks specific to business functions would be assigned to the DRMC/Departmental Risk Coordinators (RC) nominated by the concerned HOD and responsible for ensuring that the documentation required at the functional level has been developed, maintained up to date and submitted to CRO. The designated Chief Risk Officer (CRO) would be responsible for ensuring that the required documentation at the corporate level has been developed and maintained up to date with the assistance of secretary of RMC.

### 3.6 Roles & Responsibilities

Themanagement roles and responsibilities will be as follows:

| **Roles** | **Responsibilities** |
|---|---|
| **Board of Directors** | • Approve risk management policy<br>• Review and approve risk management process and provide inputs/ directions to the executive management<br>• Set 'Risk Appetite' for the Company |
| **Audit Committee** | • Lead the Risk Management initiative within the company<br>• Set standards for risk documentation and monitoring<br>• Recommend training programs for staff with specific risk management responsibilities<br>• Review and approve the risk management report including selection of critical risks to be put before the Board of Directors |

| | |
|---|---|
| **Risk Management Committee (RMC)** | • Lead the Risk Management initiative within the Company<br>• Set standards for risk documentation and monitoring<br>• Recommend training programs for staff with specific risk management responsibilities<br>• Review and approve the risk management report including selection of critical risks to be put before the Audit Committee |
| **Chief Risk Officer (CRO)** | • Implementing the risk management initiatives across the entire organization<br>• Liaise with the risk owners to coordinate flow of information and escalation of key risk issues/concerns between the DRMCs and RMC<br>• Ensure that meetings of the RMC/ DRMC are held regularly<br>• Prepare and maintain relevant documentation for the Company and present it to the Audit Committee/ Board of Directors of the company. |
| **Departmental Risk Management Committee** | • Implementing the risk management initiatives across functions<br>• Review implementation of risk management process including identification and assessment of the relevant risks at functional level<br>• Approve and submit risk documents to CRO/ RMC<br>• Provide updates to RMC on risk management |
| **Risk Owners (HODs)** | • Ensure preparation of a suitable risk mitigation plans keeping in mind the current controls mechanism in place, proposed mitigation measures and organizational priorities<br>• Ensure that the risk register/profiles are filled and key risks are escalated to the respective RMC for their approval of proposed mitigation plan<br>• 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<br>• Responsible for identifying and escalating risks to the next level<br>• 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 Chart

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

| **Roles** | **Periodicity of Meeting** | **Activities** | | | |
|---|---|---|---|---|---|
| | | **Monthly** | **Quarterly** | **Half-Yearly** | **Yearly** |
| Risk Owner | As may be required | Review and update Risk Profiles within the department and report to CRO | | | |

| | | | | | |
|---|---|---|---|---|---|
| Departmental Risk Management Committee (DRMC) | Monthly or otherwise with atleast one meeting every two months | Review of Risk Registers & Risk Profiles | | | |
| Chief Risk Officer | | | Update consolidated Risk Register (Collation of risks submitted by DRMC for escalation) | Present a detailed analysis of critical risks, risk register& risk profile to the RMC | Present top risks areas as identified by RMC to the Audit Committee/ Board |
| Risk Management Committee (RMC) | Half Yearly | | | Review of consolidated Risk Register & Risk Profile, Review of Risk Appetite Statement | |
| Board of Directors / Audit Committee | Yearly | | | | • Review of top risk areas<br>• Review the progress of Enterprise Risk Management implementation<br>• Approval of Risk Appetite Statement |

# Chapter IV:Risk Appetite

Organizations encounter risk every day as they pursue their objectives. In conducting appropriate oversight, management and the board of the Organisation are responsible for describing, how much risk is acceptable in pursuing these objectives. To fully embed Enterprise Risk Management in an organization, 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.)

## 4.1 Approach

Defining a risk appetite statement starts with analysing 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 - level 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
- Operational
- Reporting
- Compliance

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

## 4.2 Responsibility

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

The Risk Management 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.

## 4.3 DCI's Risk Appetite

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


| **High risk tolerance:** | **Medium risk tolerance:** | **Low risk tolerance:** | **Very low tolerance:** |
|---|---|---|---|
| • Potential failures in efforts for enhancing brand value<br>• Deficiencies in internal controls<br>• Deficiencies in quality, timing, and accessibility of data needed at functional level of the company.<br>• Deficiencies in financial reporting quality, timeliness, transparency and generally accepted accounting principles, etc.)<br>• Timely submission of statutory returns<br>• Malware attacks through internet/vulnerability in firewalls<br>• Inadequate implementation of preventive measure after root cause analysis of accidents and safety incidents<br>• Slow indigenization of spares. | • Quality in delivery of dredging services<br>• Improper/Under-utilization of capacities of facilities and human resources (floating and shore)<br>• Employee health and safety, grievances.<br>• Lack of periodic recruitment at entry level<br>• Certification of dredgers as per statutory requirements and compliance accordingly.<br>• Delays in vendor payments.<br>• Improper planning to supply of fuel & lubes<br>• Vendor performance<br>• Irregular monitoring of periodic preventative maintenance. | • Delays in project execution<br>• Potential Failures in the pursuit of diversification and expansion of existing business<br>• Timely release of payments by clients<br>• Delays in dry dock repairs of dredgers<br>• Non closure of NC's before due date<br>• Delay in supply of spares and parts | • Violations of legal and regulatory requirements including code of ethics / fraud prevention policy of the company.<br>Lack of refined data base on present market as well as on potential competitors |

# Chapter V: Risk Management Process

## 5.1 Risk Identification

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

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

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

All identified risks shall be updated in a risk register. Risk registers shall be reviewed half-yearly by the RMC which are to be updated by the respective Departmental Risk Management Committees to ensure pertinence of the risks listed. Risks that would have ceased shall also be closed appropriately. The CRO and Risk Owners shall ensure that the departmental risk registers are reviewed and updated monthly.

## 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 combination of likelihood of occurrence and the magnitude of impact provides the risk level. The magnitude of impact of an event (shall it occur), 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:

| 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:

| Levels | Descriptors |
|---|---|
| 5 | Very High Impact |
| 4 | High Impact |
| 3 | Moderate Impact |
| 2 | Low Impact |
| 1 | Very Low Impact |

Risk assessment criteria for DCI is given as per Annexure V

### 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:**

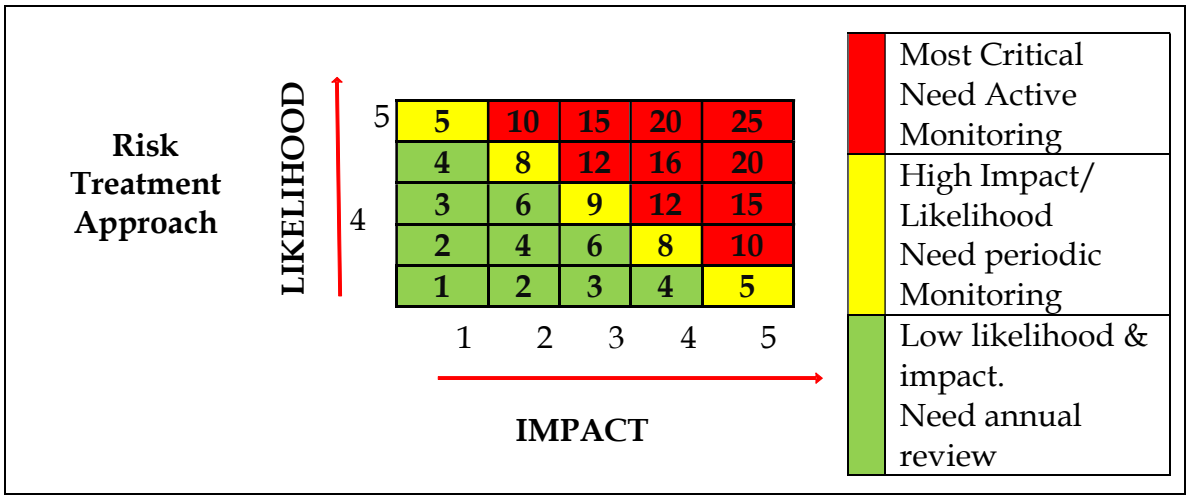
| | **Likelihood (A)** | **Impact (B)** |
|---|---|---|
| Participant 1 | 2 | 5 |
| Participant 2 | 3 | 5 |
| Participant 3 | 4 | 5 |
| Total | 9 | 15 |
| **Group Score i.e. Simple Average (Total/No of Entries)** | **3** | **5** |
| **Combined Score (Group Score A x Group Score B)** | **15** | |

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 action 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 6and less than12)

- 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 DCI in prioritizing risk treatment strategies to ensure that appropriate attention is given to risks based on their criticality and that the resources of DCI are effectively utilized in managing these risks.

### 5.4 Risk Treatment/Action Plan

The risk mitigation plan adopted by DCI 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 treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Treatment options may include:

- Avoidance–Exiting the activities giving rise to risk. Risk avoidance may involve exiting a project, declining expansion to a new geographical market etc.
- Acceptance – No action is taken to mitigate the risk or reduce the likelihood or impact.
- Reduction –Developing mitigation plan to reduce 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 IV**. The profile contains details of the risk, its contributing factors, risk scores, controls documentation, and specific and practical action plans. Action 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 treatment process. For risks considered to be "acceptable" risk profile will be developed with mitigation plan as accepted and no further actions required.

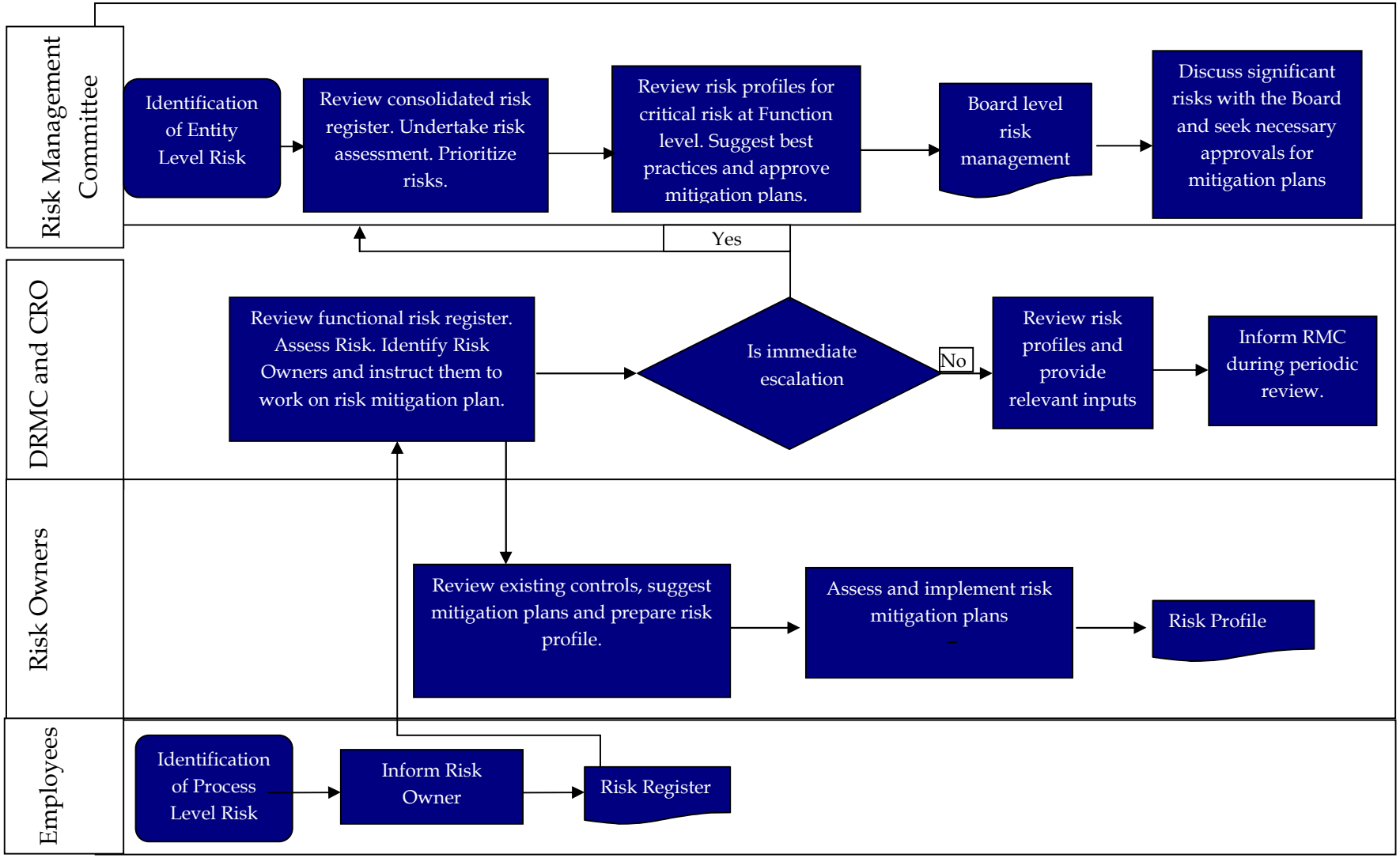
### 5.5 Escalation of risks

An effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately should be instituted. Every employee of the DCI has responsibility of identifying and escalating the risks to appropriate levels within the DCI. After the risk is identified upward escalation of the same will be as below:

- Departmental Risk management committee head to select risks to be escalated which primarily will be of following types:
  - Critical risks relevant to the function wherein the complete mitigation is not possible at DRMC level
  - Critical interdependent risks wherein intervention of RMC/Audit Committee/ 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 RMC/Audit Committee/ Board for integrated response/mitigation plan.
- The CRO shall select risks to be escalated to RMC based on the inputs received from respective DRMCs. This would include:
  - Risk submitted by individual DRMCs as critical for their respective function
  - For critical interrelated risks the CRO need to present to the RMC, an aggregate/consolidated view of the risks after thorough analysis and consultation with DRMC heads of relevant department

- RMC will review the risks submitted by CRO and will identify and escalate strategic risks to the Board. Overall escalation and information flow within the Company will be as follows:

**Process of Escalation of Risk across Organization Levels**



### 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 treatment options.

Risk review aims at assessing the progress of risk treatment action 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 RMC.

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

### 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 the client/sub contractor.

## Chapter VI: Reporting

A report comprising of top critical risk areas (including mitigation plans) duly approved by the RMC, shall be placed before the Audit Committee/Board. The format of such report may be as suggested by the board. On yearly basis, the Audit Committee/Board would review the progress of risk management implementation (including areas such as training requirements, process improvisation etc.).

## Annexure I: Illustrative list of risk categories

| S.No | Risk Classes/Baskets | Definitions |
|---|---|---|
| 1. | Strategy/ Business Development | Risks associated with strategy development, strategic alliances, business continuity plan, business model, growth, reputation, innovation and performance targets. |
| 2. | Marketing/Tendering, Contract Management | Risks associated with marketing/tendering process and documentation, competition, conflicts, compliance, quality, delivery and fulfillment of obligations of contracts. |
| 3. | Operations/Project Management | Risk associated with core dredging operations. Risk associated with planning, organizing and managing resources to bring about successful completion of specific project goals and objectives. |
| 4. | Technical | Risks associated with dry dock planning, maintaining health of the dredgers |
| 5. | Materials | Risks associated with procurement process, internal and external logistics and transportation, quality controls, outsourcing and vendor relationships |
| 6. | Finance | Financial risks include risks associated with capital structuring, capital allocation, financial management of revenue, debtor's management, forex, hedging and preparation of financial statements. |
| 7. | Human Resource (HR) | Risks associated with culture, organizational structure, recruitment, performance management, remuneration, learning & development, retention including supporting systems, processes, and procedures. |
| 8. | Budgeting/ Forecasting | Risks associated with, budgeting, management reporting and cost/expenditure management. |
| 9. | Information Technology/Security | IT risk include issues like IT strategy, networks, support systems, interfaces, data reliability, access controls disaster recovery<br><br>Risk associated with Cyber security, data loss, fraud, system outages, breach of confidentiality, legal/regulatory violations, as well as data integrity. |
| 10. | Environment, Health and Safety | This category includes risks related to environment pollution, safety of resources, employees' health, etc., |
| 11. | Legal& Regulatory Compliance | Failure of infrastructure processes, systems, and resources to support legal and regulatory requirements. |

| S.No | Risk Classes/Baskets | Definitions |
|---|---|---|
| | | Risk relating to noncompliance with tenders, legislation, regulations, internal policies and procedures. |
| 12. | External Factors | The risks associated with external factors like political, economic /markets, social, technological, legal and regulatory, fraud, and al Environmental Social Governance pose threat to the organization. |

This list may be modified by CRO in future to add/modify risk categories that may emerge.

## Annexure II: Template for Risk Register

| Sl. No. | Dept Risk Management Committee | Risk Category | Risk Statement | Contributing Factors | Impact Score | Likelihood Score | Total Score | Risk Rating | Risk Owner | Existing Controls | Proposed Mitigation Plans | Mitigation Plan Owner 1 | Mitigation Plan Owner 2 | Target Date | Status | Date of deletion / addition | Remarks |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | |

[Space left blank intentionally]

## Annexure III: Risk Management Meeting Template

| | |
|---|---|
| Committee | RMC/ DRMC |
| Date & Time | |
| Location | |
| Participants | 1. Name (Designation)<br>2. Name (Designation)<br>3. Name (Designation)<br>4. Name (Designation) |
| Agenda: | |
| | |
| Summary of Discussion | |
| Significant Points Discussed: | |
| Proposed Action Items | |

## Annexure IV: 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<br>• Factor 2 .....<br>• Factor n | | • Control 1<br>• Control 2 .....<br>• Control n | | | |
| **Type of Risk Rating** | **Current Review** | | **Last Review** | | | |
| **A. Likelihood Rating [1-5]:** | (Rating score of last review) | | (Rating score of current review) | | | |
| **B. Impact Rating [1-5]:** | (Rating score of last review) | | (Rating score of current review) | | | |
| **Overall Risk Rating (A*B):** | (Rating score of last review) | | (Rating score of current review) | | | |
| **Risk Type** | (Critical/ Cautionary/ Acceptable) | | | | | |
| **RISK MITIGATION PLAN** | | | | | | |
| **Sr. No.** | **Description** | **Target Date** | **Target Date Decided By** | **Responsibility** | **Submit Date** | **Comments** |
| 1. | | | | | | |
| 2. | | | | | | |
| **Signatures:**<br>_____ _____ _____<br>**(Risk Owner)** **(Risk Coordinator)** **(Chairman- Risk Management Committee)** | | | | | | |

## Annexure V: 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 within 1% on revenue | Impact > 1% upto 3% on revenue | Impact > 3% upto 5% on revenue | Impact >5% upto 10% on revenue | Impact > 10% on revenue |
| | Impact < 2% on profit before tax | Impact > 2 to 5% on profit before tax | Impact > 5% to 8% on profit before tax | Impact >8% to 10% on profit before tax | Impact> 10% on profit before tax |
| Reputation | • Minimal local media attention<br>• Short term recoverability of reputation<br>• Minimal impact on ability to raise finance<br>• Minimal impact on DCI brand image | • Regional media attention<br>• Loss of reputation for a moderate period of time<br>• Relatively small impact on ability to raise finance<br>• Minor impact on DCI brand image | • Sustained negative regional media attention<br>• Loss of reputation for a long period of time<br>• Major impact on ability to raise finance<br>• Major impact on DCI brand image | • Negative national media attention<br>• Loss of reputation for a moderate period of time<br>• Significant impact on ability to raise finance<br>• Significant impact on DCI brand image | • Sustained negative national media attention<br>• Significant loss of reputation for a long period of time<br>• Critical impact on ability to raise finance<br>• Severe impact on DCI brand image |
| Regulatory/ Legal | • Routine Issues raised by regulatory authority | • Caution/ Instructions from regulatory authority | • Penalties/ Intensive scrutiny | • Heavy penalties/ restrictions on activity | • Prosecution/ loss of rights to operate |
| Employees | • Isolated staff dissatisfaction | • General staff morale problems and increase in turnover | • Widespread staff morale problems and moderate turnover | • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice | • Multiple senior leaders leave |
| Customers | • Customer attrition of < 1 % | • Customer attrition of 1 to 2 % | • Customer attrition of > 2 < 5 % | • Customer attrition of <> 5 < 10 % | • Customer attrition of > 10 % |

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 |