Risk Management Policy

Kamarajar Port Limited

January 2015

1 Contents

2 Introduction and Risk Objectives

Kamarajar Port Limited (KPL or "the Company") recognizes that risk is inherent to any business activity and that managing risk effectively is critical to the immediate and future success of the Company.

Risks are events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. The exposure to the consequences of uncertainty constitutes a risk. The Chinese word for risk contains two characters, danger and opportunity. If we remove all danger or downside risk, then we create barriers to exploit opportunities or benefits. Conversely, if we ignored all downside risk or do not manage it effectively then we increase likelihood of a major negative effect. To manage such contradictions Risk Management Policy should be in place.

The Company is a public limited company incorporated under the Companies Act, 1956. Further, KPL is also a Central Public Sector Enterprise (CPSE) whose shares are held by Government of India 67% and Chennai Port Trust 33%. Therefore, it is required to abide by the guidelines on corporate governance for CPSEs by the Department of Public Enterprises (DPE).

According to Section 134(3) (n) of the Companies Act, 2013: There shall be attached to (financial) statements laid before a company in general meeting, a report by its Board of Directors, which shall include— (n) a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the Board may threaten the existence of the company;

According to DPE guidelines for CPSEs, 2010, "the company shall lay down procedures to inform Board members about the risk assessment and minimization procedures. These procedures shall be periodically reviewed to ensure that executive management controls risk through means of a properly defined framework. Procedure will be laid down for internal risk management also."

The Company, through this Risk Management Policy, presents an enterprise-wide approach to ensure that key aspects of risk that have an enterprise-wide impact are considered in its

conduct of business. This policy document serves as a guideline for respective components of risk which have a common resonance across the company.

The Risk Management Policy provides entity level risk guidelines encompassing key risk areas across the company such as Business Risk, Operational Risk, technology risk and Strategic and Reputation risk.

2.1 Objective

The main objective of this policy is to ensure sustainable business growth with stability and to promote a pro-active approach in reporting, evaluating and resolving risks associated with the business.

Risk Management in the Company provides a framework to identify, assess and manage potential risks and opportunities. It provides a way for managers to make informed management decisions.

Some of the objectives of a Risk Management Framework are given below.

- A focused approach in identifying the obstacles & managing them will help the Organizations to perform better.
- Introduce a structured risk management initiative across the Organization to identify potential risks that may adversely affect the objectives of the Organization, plan for their mitigation with specific responsibility.
- Implement such a plan with a targeted date and review periodically.
- Improves strategic decision making;
- Improves business performance;
- Reduces operational surprises and losses;
- Promote a more innovate and less risk averse culture;
- Improves deployment of capital;
- Provide a sound basis for integrated risk management and internal control as components of good corporate governance;
- Seizing opportunities.

2.2 Risk Management Principles

- The principles contained in this policy and strategy will be applied at both corporate and operational levels within the organization.
- The Company's Risk Management Policy and Strategy will be applied to all operational aspects of the Company and will consider external strategic risks.
- Our positive approach to risk management means that we will not only look at the risk of things going wrong, but also the impact of not taking opportunities or not capitalizing on corporate strengths
- Responsibility for identifying and managing risks is a routine part of the role of management at all levels, including the identification and regular monitoring of key risk indicators;

2.3 Components of a Sound Risk Management System

The risk management system at the Company has the following key features:

- Active board and senior management oversight
- Appropriate policies, procedures and limits
- Comprehensive and timely identification, measurement, mitigation, controlling, monitoring and reporting of risks
- Appropriate management information systems (MIS) at the business level
- Comprehensive internal controls in accordance with current regulations
- A Risk Culture and communication

2.4 Risk Management Policy Statement

To protect and add value to the organization and its stakeholders through supporting the organization's objectives by:

- Providing a framework for an organization that enables future activity to take place in a consistent and controlled manner
- Improving decision making planning and prioritization by comprehensive and structured understanding of business activity, volatility and project opportunity /threat
- Contributing to more efficient use / allocation of capital and resources within the Organization
- Developing and supporting people and the organization's knowledge base

2.5 Benefits of Risk Management

Risk management enables the company to meet values and deliver upon its objectives. Application of a consistent and comprehensive risk management process will:

- Increase the likelihood of achieving strategic and business objectives;
- Encourage a high standard of accountability at all levels of the organisation;
- Support more effective decision making through better understanding of risk exposures;
- Create an environment that enables it to deliver timely services and meet performance objectives in an efficient and cost effective manner;
- Safeguard assets – human, property and reputation; and
- Meet compliance and governance requirements.

2.6 Terms and Definitions

Terms and definition are included in Annexure for reference.

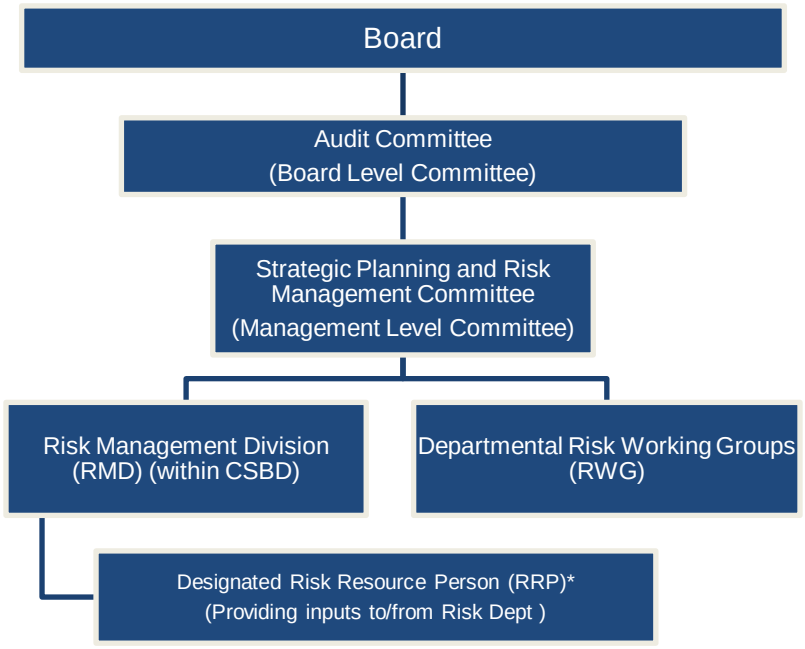
3 Risk Organisation Structures

An organisation's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well-defined roles and responsibilities.

Risk governance signifies the manner in which the business and affairs of an entity are directed and managed by its Board of Directors and executive management. It also provides the structure through which the objectives of an organization are set, the strategy for attaining those objectives is determined and its performance is monitored, while ensuring, that the interests of the different stakeholder communities are taken into cognizance and acted upon.

In order for risks to be effectively managed, it is essential to have people behaving in a way that is consistent with the organisation's approved approach. This indicates that risk management is not merely about having a well-defined process but also about effecting the behavioural change necessary for risk management to be embedded in all organisational activities.

The risk organization structure emanates from the governance principles. The risk organization structure for the Company is as depicted below. This structure illustrates that risk management is not the sole responsibility of one individual but rather occurs and is supported at all organisational levels.



*Each department will nominate one of its executives as RRP to maintain Risk Register and liaison with Risk Manager on risk issues of the department. All correspondences from RRP would be routed through the Head of the Department. Risk Manager would seek information from RRP through the HOD also.

3.1 Roles and Responsibilities

3.1.1) Board

The Company's risk management architecture is overseen by the Board of Directors (BOD) and policies to manage risks are approved by the Board. The responsibility of understanding the risks run by the firm and ensuring that they are appropriately managed is placed with the Board of Directors. The Board of Directors has the duty to shareholders to ensure that requisite systems, practices and culture are in place to manage all risks to which the firm is exposed.

The Board is responsible, in particular, for ensuring that there are adequate risk management arrangements and a sound system of internal control.

Responsibilities of the Board

The responsibilities of the members of the Board with respect to risk management can be summarised as follows:

- Ensure that the organization has proper risk management framework
- Define the risk strategy and risk appetite for the company
- Approve various risk management policies including the code of conduct and ethics
- Ratify any changes to the risk management framework including those necessitated by change of regulatory environment, launch of new products/services or business practices.
- Maintain oversight and evaluate the risk management function
- Ensure that senior management takes necessary steps to identify, measure, monitor and control these risks
- Ensure that senior management monitors the effectiveness of internal control system

- Help in identifying risk, assessing the risk, policies / guidance notes to respond its risks and thereafter frame policies for control and monitoring.
- Developing and communicating organizational policy and information about the risk management programme to all staff, and where appropriate to our associates / suppliers / contractors etc.;
- Setting policies on internal control based on the organisation's risk profile, its ability to manage the risks identified and the cost/ benefit of related controls; and
- Seeking regular assurance that the system of internal control is effective in managing risks in accordance with the Board's policies.
- The Board delegates to the Strategic Planning and Risk Management Committee the responsibility of the day to day execution of the risk management policies so that the risk is effectively managed in the Company.

3.1.2) Audit Committee

The Audit Committee assists the Board in carrying out its oversight responsibilities relating to the Company's (a) financial reporting process and disclosure of financial information in financial statements and other reporting practices, b) internal control and risk management (c) compliance with laws, regulations, and ethics (d) financial and risk management policies.

The Audit Committee assists the Board in its oversight responsibilities relating to risk management in the following areas:

(a) identification of risks

(b) determination and ranking of risks

(c) risk mitigation measures

The Audit Committee is governed by Audit Committee Charter that outlines its roles and responsibilities.

3.1.3)Strategic Planning and Risk Management Committee (SPRMC)

The Strategic Planning and Risk Management Committee (SPRMC) is responsible for managing all types of risks in the Company. The Board of Directors approves the broad risk management policies with the day–to–day decisions delegated to the SPRMC so that risk can be effectively managed. The SPRMC is empowered to delegate limits at appropriate levels down the hierarchy in various business units.

The SPRMC is the key management level Committee that would drive risk management at KPL. It would meet monthly to discuss key risk and mitigating actions taken by the company.

The SPRMC would carry out the following roles:

(i) review Long Term Business Plan (LTBP) of the Company and recommend appropriate modifications/changes thereto for approval by the Board

(ii) set action plan priorities in line with LTBP duly incorporated in Annual Plans

(iii) identify projects integrated to strategic goals and objectives in line with LTBP and monitor their implementation/execution

(iv) administer Risk Management Framework (RMF) to identify and mange risks and monitor risk mitigation plans from time to time.

One of the key roles of the SPRMC would be project risk management. To enable this function, all projects that are planned during the year with estimated value over a threshold limit as decided by the Board shall be evaluated at the SPRMC.

.A Project with estimated value beyond SPRMC authority shall be approved by the Board on the basis of recommendation from the SPRMC.

A designated project manager shall be responsible for executing each project. The designated project manager shall ensure that a detailed proposal/project report is submitted for discussion at the department level Risk Working Group (RWG) for identifying risks and putting in place risk mitigation plans to be duly incorporated in the proposal/project report before submitting the same for approval by the appropriate authority as per DOP.

RWG shall monitor progress of execution of all projects and submit reports thereof to SPRMC. Such monitoring reports for projects up to Rs 5 crore shall be submitted to SPRMC on a quarterly basis and for projects above Rs 5 crores on a monthly basis.

Charter

The Committee's Charter is provided as Annexure - A.

3.1.4)Risk Management Division

The Risk Management Division is the key division which would implement and coordinate the risk function as outlined in this policy on an ongoing basis. It would act as the central resource division for administration of RMF by SPRMC to mitigate the risks to the Company's business as it may evolve over time.

Risk Management Division (RMD) is part of the CSBD Department. A full time employee or external consultant on a contract basis would act as the Risk Manager. The Risk Manager would oversee implementation of the RMF, coordinate with the Risk Resource Person in each department, discharge secretarial services to the SPRMC, update risk management policy and procedures and implement management and development activities relating to the risk function.

Responsibilities of the Risk Management Division / Risk Manager

- Develop and recommend to the SPRMC and the Board of Directors, a risk profile for the Company;
- Develop and implement the Company's risk management strategy;
- Develop, enhance and implement appropriate risk management policies, procedures and systems
- Work with risk owners to ensure that the risk management processes are implemented in accordance with agreed risk management policy and strategy
- Review risks and risk ratings of each department in coordination with departmental Risk Resource Persons (RRPs)
- Collate and review all risk registers for consistency and completeness

- Provide advice and tools to staff, management, the Executive and Board on risk management issues within the organisation, including facilitating workshops in risk identification
- Oversee and update organisational-wide risk profiles, with input from risk owners and RRPs
- Ensure that relevant risk information is reported and escalated or cascaded, as the case may be, in a timely manner that supports organisational requirements
- Secretary to SPRMC

3.1.5)Departmental Risk Working Groups (RWG)

The purpose of the departmental Risk Working Group (RWG) is to bring cohesiveness in functioning of the department by sharing work related knowledge and risk concerns among managers. This will help increase efficiency of the department to better manage risks and better manage projects. .

Constitution

Departmental RWG shall be created for each Business Function. Presently, there are five functional departments- Operations, Marine Services, Corporate Strategy & Business Development, Finance and Secretarial & legal. Members of the RWG shall be all Divisional Heads/key staff including Risk Resource Person (RRP) of the department

Periodicity

RWG should meet weekly/fortnightly once on a scheduled day.

Responsibilities

Broad roles and responsibilities of the RWG are as follows

- Review project proposals/project reports as to scope, cost, schedule, , quantity, quality and method of execution
- Identify risks in projects and general functioning of the department and risk mitigation plans

- Review of tender and contract scope, terms and condition
- Review progress of project execution
- Review check lists for project monitoring and port facility/maintenance contract monitoring
- Periodic Review of Port Facilities related inspection reports
- Review Risk Register of the department to ensure that all identified risks and their risk mitigation plans included
- Review assessment of inherent as well as residual risk ratings and action plans
- Monitor risk mitigating action plans

3.1.6) Risk Resources Persons (RRP) within Departments

All personnel forming a part of the Risk Organisation Structure have to be trained on the company's risk management system. Additionally, a Single Point of Contact (SPOC) will be designated by each department to act as the Risk Resource Person (RRP) to coordinate with Risk Manager in terms of risk management activities. All correspondences from RRP would be routed through the Head of the Department. Risk Manager would seek information from RRP through the HOD also.

Specifically, broad roles and responsibilities of the RRP within functional departments are as follows

- Comply with Company standards which relate to particular types of risks;
- Manage the risk they have accountability for
- review the risk on a regular basis
- identify where current control deficiencies may exist;
- act as secretary to the RWG of the department
- Update risk registers periodically and provide information about the risk when it is requested

4 Risk Management Framework

Risk Management Framework involves a continuous management and monitoring of risks across the Company. Hence, the process is a dynamic framework to enable risk management effectively and efficiently. The risk management process covers the steps to be taken by the Company's management and staff in the process of identifying, assessing, mitigating and treating the risks the company is exposed to.

A risk management framework aims to assist an organisation to manage its risks effectively through the application of the risk management process at varying levels and within specific contexts of the organisation. Such a framework should ensure that risk information derived from these processes is adequately reported and used as a basis for decision making at all levels.

> *A risk management framework is defined as a Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation*

4.1 Risk Appetite

The Board will approve the risk profile or appetite of the Company in material risk areas. The objective of risk appetite statements is to restrict the overall risk levels of the Company based on pre-defined strategies. Within the overall risk appetite defined, risk tolerance limits will be set.

Risk appetite is communicated through the Company's strategic plans. The Board and management monitor the risk appetite of the Company relative to the Company's actual results to ensure an appropriate level of risk tolerance throughout the Company

Some of the elements that could be considered to define risk Appetite are:

- shareholder and investor preferences and expectations;
- expected business performance (return on capital);
- the capital needed to support risk taking;
- the culture of the organisation;
- management experience along with risk and control management skills;
- longer term strategic priorities.

The Board encourages the taking of controlled risks, the grasping of new opportunities and the use of innovative approaches to further the interests of the organization and achieve its objectives provided the resultant exposures are within the organisation's risk tolerance.

Acceptable risks

- All personnel should be willing and able to take calculated risks to achieve their own and the Company's objectives and to benefit the Company. The associated risks of proposed actions and decisions should be properly identified, evaluated and managed to ensure that exposures are acceptable.
- Within the Company, particular care is needed in taking any action which could:
    - Impact the reputation of the Company;
    - Impact performance;
    - Undermine the independent and objective review of activities;
    - Result in censure / fine by regulatory bodies; or
    - Result in financial loss

4.2 *Current Risk Appetite Statements*

The Company's management has defined the following as the risk appetite. These are reviewed annually and placed to the Board for approval and implementation.

Criterion	Risk Appetite Statement	Early Warning Levels	Frequency of Review
Market Share	Regional Market share (amongst immediate peer companies) not to be below 25%	30%	Yearly
Capacity	Minimum Annual (Last 3 years average) Capacity addition to be atleast 5 MTPA	N/A	Yearly
Infrastructure	Planned infrastructure progress to be atleast 75% of budgeted expenditure	N/A	Yearly

For the purpose of Market share, peer group consists of Chennai Port, Katupali (L&T), Krishnapatnam and Karaikal ports.

Any breaches to the Risk Appetite require reasons for the breach as well as planned action plan to bring back operations to comply with the risk appetite statements. A note containing planned remedial actions is placed to the SPRMC soon after the breach. Minutes of the SPRMC are placed to the Audit Committee for review and approval.

4.3 *Risk Management and Budgeting*

- Key Risk Management inputs, specifically the risk appetite and risk tolerance are key inputs in setting up business strategies for the forthcoming years. Any business strategies or investment decisions, product launches are considered within the overall risk appetite.
- The Board of Directors reviews major investment decisions and initiatives after getting an understanding of the current risk profile of the organisation and inherent risks of the new investment or initiative.

5 Risk identification

Risk identification forms the core of the Risk Management system. Multiple approaches for risk identification are applied to ensure a comprehensive Risk Identification process.

The organization should identify sources of risk, areas of impacts, events and their causes with potential consequences. Comprehensive identification is critical, because a risk that is not identified here will be missed from further analysis.

The purpose of the risk identification activity is to generate a comprehensive list of events and sources of risk that may impact the Company's risk profile. The risk identification process should capture all significant risks and identify potential threats facing the organisation. The process includes, but is not limited to, a review of key assumptions, milestones, deliverables and inter-relationship between risks.

Risk Identification is performed at strategic functions at the entity level as well as at the process level for each function and process. A separate categorization is made for the type of key risk to better align efforts towards these risks. Process level risks are better managed by the Business functions whereas Strategic and entity level risks are managed jointly by Business Units and Senior Management in the Corporate Office.

Risks that are identified are also categorized in broad categories to better reflect on which areas are of concern for the Company. The categories are part of the Risk Register format. A list of standard risk categorization is given in Annexure – B.

5.1 Business Functions

For the purpose of risk identification and to ensure that all risks across each business are captured, the Company identified the business functions and processes important for this purpose. The following is the list of business functions for which Risk identification is carried out.

a) Compliance, Secretarial and Legal
b) Finance
c) Corporate Strategy & Business Development - Public Relations
d) Corporate Strategy & Business Development - Human Resources
e) Marine services – Electronic Data Processing
f) Marine Services - Safety
g) Marine Services - Services
h) Marine Services - Survey & Dredging

i) Operations - Buildings
j) Operations - Corporate Social Responsibility
k) Operations - Electricals
l) Operations - Environment
m) Operations - Estate
n) Operations - Projects
o) Operations - Roads, Berths & Break Waters

5.2 Risk Description

A risk description helps in understanding the nature and quantum of risk and its likely impact and possible mitigation measures. Risk descriptions for each of the risks identified in the Risk Matrix are to be documented and recorded in a structured format in each area where the risk is identified. Risk descriptions are incorporated into the Risk Register.

5.3 Risk Register

For the purpose of consolidation of material risks, all the outputs of the various risk identification and assessment processes are reviewed by the Risk Manager in collaboration with Business Heads. These are aggregated in a Risk Register capturing the key risk, mitigating controls and other details about the particular risk. A Risk Register is to be maintained by the company in the prescribed format which contains a listing of all the risks identified by the company.

The format adopted by the company of such a Risk Register is given in Annexure - C.

5.4 Maintenance and Regular updates to Risk Register

Risk Manager is the owner of the Risk Register and ensures that it is current at all times. For this purpose, informal interactions with Departmental Heads/RRPs are likely to identify new or emerging risks that are considered key. Risk Resource Person (RRP) in each department facilitates update of risks in the risk register for the department and forwards to the Risk Manager. These are updated by the Risk Manager into the consolidated Master Risk Register on a continuous basis.

In addition, a formal risk identification process, as outlined above, in the form of a workshop or similar methodology, is performed half yearly to review and revise the Risk Register. For this purpose, Senior Management and Departmental Heads are engaged in an active dialogue to discuss these risks.

Revised Risk Register is circulated for final approval, once other risk management steps have been completed.

6 Risk Assessment and Risk Rating

For all key risks identified during the Risk Identification process, a qualitative and quantitative assessment is carried out. Risk assessment involves different means by which to grade risks in order to assess the possibility of their occurrence and extent of damage their occurrence might cause. Likelihood rating and impact rating is as per the Rating parameters defined by the Company. The current rating parameters are outlined in Annexure - D.

Risk Assessment and rating methodologies take a systematic approach to determine the impact of occurrence of a risk and its likelihood of happening. In brief, the assessment involves following key steps

- Rating of each risk as per the probability of the risk event occurring
- Rating the risk as per the financial impact of that risk event should the risk event occur. The two parameters provide the quantitative element to risk assessment.

The process of Risk Assessment shall cover the following:

a) **Risk Identification and Categorisation** – the process of identifying the company's exposure to uncertainty classified as Strategic / Business / Operational.

b) **Risk Description** – the method of systematically capturing and recording the company's identified risks in a structured format

c) **Risk Estimation** – the process for estimating the cost of likely impact either by quantitative, semi-quantitative or qualitative approach.

Once the risks are analysed, these can be plotted on a heat map and shared with the SPRMC or CMD. A format of the heat-map is provided below.

	Risk Matrix		
IMPACT			
High (Significant)	**3**	**6**	**9**
Medium (Moderate)	**2**	**4**	**6**
Low (Insignificant)	**1**	**2**	**3**
	Low (Unlikely)	Medium (Possible)	High (Likely)
	Beyond 3 Years	Once in 3 Years	Once in 1 Year
	PROBABILITY OF OCCURANCE		

As part of the above risk assessment, key risks falling in the red zone will be subject to greater risk management by way of monitoring and mitigating controls. Accordingly, risks with a residual risk rating score of 6 and 9 are considered significant risks which require risk mitigation on a priority basis.

6.1 Risk Assessment Techniques

Risk assessment is a fundamentally important part of the risk management process. In order to achieve a comprehensive risk management approach, organization needs to undertake suitable and sufficient risk assessments.

A range of the most common risk assessment techniques is set out in the Table below for guidance.

Technique	**Brief Description**
Questionnaires and checklists	Use of structured questionnaires and checklist to collect information to assist with the recognition of the significant risks
Workshops and brainstorming	Collection and sharing of ideas and discussion of the events that could impact the objectives, stakeholder expectations or key dependencies
Inspections and audits	Physical inspections of premises and activities and audit of compliances with established systems and procedures
Flowchart and dependency analysis	Analysis of processes and operations within the organization to identify critical components that are key to success

7 Risk Prioratisation and Mitigation

7.1 Risk Prioritization

After the risk assessment is complete, it is the responsibility of the Risk Management Function to prioritize the key risks to determine which risk are considered key and need to be addressed on a priority basis. In fact, this prioritization is one key phase that will ensure successful risk management program implementation.

Prioritization of risks involves using final ratings. The risks are plotted on a 3X 3 matrix, given above to identify which risks are materials from a corporate perspective. For this purpose, the materiality scales are used to identify the severity and likelihood of these risks. All risks that fall in the red zone are considered high risk and require immediate attention in terms of risk management. The Company proposes to categorize all “High Risk (red zone) and some important Medium risk (Yellow zone) risks” as high priority. These will be tracked on a constant basis as per Risk Monitoring process outlined below.

The findings of risk prioritization are presented to SPRMC and Business Units on a regular basis.

7.2 Risk Mitigation Process

Once the top or critical risks are listed, appropriate risk mitigation and management efforts to effectively manage these risks are identified. Risk mitigation strategy usually involves identifying a range of options for treating risk, assessing those options, preparing and implementing risk treatment plans. The risk mitigation strategies may include managing the risk through implementation of new internal controls, accepting certain risks, taking insurance, and finally avoiding certain activities that result in unacceptable risks. Proposed actions to eliminate, reduce or manage each material risk will be considered and agreed as part of the business function meetings (RWG meetings) or during the SPRMC meeting.

7.3 Action Plan and Status

A risk mitigation action plan is outlined for all priority risks in the high and medium categories. Senior Management and Business Heads design an action plan to mitigate and monitor each of these key risks.

An action plan and status reporting is implemented to log actions proposed to mitigate risks and track status of Evidence, of regular review and monitoring of the profile and action plan. The action plan and status reporting is reported quarterly to SPRMC to update on the status of mitigation efforts.

Format of Action Plan

Action plan information forms part of the Risk Register and is not maintained separately. When reporting on the Action plan, Risk Manager reports the following information necessary for review of Action plan. The following information is reported to SPRMC for all Risks with Residual Risk rating levels of 4, 6 and 9.

KAMARAJAR PORT LIMITED - Action Plan								
Risk. No.	Risks	Causes	Risk Category	Residual Risk Rating	Proposed Remedial Action for Risk Mitigation	Action Owner	Action Due Date	Status of Action Plan
Business Function								

8 Risk Reporting and Monitoring

An enterprise-wide integrated Risk Management Information System (MIS) needs to be implemented by the company. Such information is needed at all levels of the organization to identify, assess and respond to future occurrences of risk events. Pertinent information from both internal and external sources must be captured and shared in a form and timeframe that equips personnel to react quickly and efficiently.

The Company's MIS provides the Board and senior management in clear and concise manner timely and relevant information concerning the risk profile. The MIS is capable of capturing major policy breaches and effective in promptly reporting such breaches to senior management, as well as to ensure that appropriate follow-up actions are taken.

Given the small size of the company, most of the internal reporting and day to day interactions between senior management and Business Functions ensures that senior management is aware of key risks and unusual incidents or loss events. In addition to this, formal risk reporting has been introduced to highlight risk profiles, trends, key issues and effectiveness of RMS.

The ongoing business success of the Company depends to a great extent on risk awareness and the ability to manage risks. This requires transparency of all risk taking activities and thus an effective risk reporting system. The following is a summary of the Risk Management Reporting that communicates the risk profile and risk mitigation efforts.

8.1 Company and Business Risk Profile

In order to manage risks, key risk dashboards are implemented to review risk levels at a Company level as well as at business function levels. For this purpose, a departmental Risk Level Dashboard as given in Annexure - E is reported on a quarterly basis to the SPRMC for review along with the updated Risk Register.

8.2 Risk Monitoring and Risk Calendar

As the risk exposure of any business may undergo change from time to time due to continuously changing environment, the updation of the Risk Matrix will be done on a regular basis.

The Risk Manager shall maintain a risk calendar that outlines the frequency of performance of various risk management activities. The current risk calendar is attached as Annexure - F.

8.3 Quarterly Review of Risk Management Framework

Progress on implementation of Risk management system is reviewed by the SPRMC on a quarterly basis and submitted to the Audit Committee/Board. As part of the Board Reporting Package, Risk profile of departments (Risk Level Dashboard: Annexure - E) and a summary of high risks (rating 6 & 9) in the format given in Annexure – J, having been reviewed by the SPRMC, would be presented to the Board.

9 Specific Guidelines for Risk Management

9.1 Project Risk Management

KPL, primarily a port infrastructure provider faces significant sector specific and location specific risks in implementation of Projects. Project Risk Management assumes greater significance in the wake of inherent risks associated with Social, Environment, Geotechnical conditions etc. In addition there are uncertainties, often linked to political pressures and negative publicity related to environmental and social aspects, often resulting in public disturbances. All these risks cause time and cost overrun. Similarly, for Plants under operation there are threats of accidents, machine break down, generation loss etc. In addition marine risk may affect the revenue. For sustainable development all these risks need to be effectively handled.

The Company undertakes various high value projects that normally extend beyond the short and medium term. Timely and successful completion of these projects is critical for the Company in terms of throughput as well as maintaining competitive advantage.

In order for comprehensive project risk management, the Company has introduced Risk Working Groups (RWG) that will be the working arm of the SPRMC. During these RWG meetings, key project risk and issues will be discussed and required action plans and decisions taken.

A Project Risk Summary Dashboard will be provided to SPRMC on a quarterly basis as per format given in Annexure - G.

9.2 Internal Audit and Internal Controls

The Company has adopted a Risk Based Internal Audit approach whereby internal controls will be strengthened by performing internal audits focusing on specific risk areas. An annual Audit plan shall be approved by the Audit Committee. Internal Audit and Risk Management will supplement efforts for an integrated risk management outcome.

Section 177(4) (vii) of the Companies Act, 2013 requirement:

"Every Audit Committee shall evaluate the internal financial controls and risk management systems of the Company"

9.3 Incident Reporting / Unusual Events Reporting

A source of risk identification is the occurrence of actual loss or risk incidents during the course of the business. These incidents that are not part of business as usual are a good tool to identify the types of risks that can occur within the company. As such, the company has implemented the incident reporting process.

Incidents occur as part of day to day business and these incidents are required to be reported to the Risk Management Division as part of risk identification. Such events with significant risks are being reported by the different businesses and functions on a regular basis to understand the adequacy of the risk management activity and evaluate the effectiveness of the processes.

The process requires all functional units to report all kinds of events which are unusual in nature and occurring in their daily course of activities.

Detailed procedures adopted by the Company for Incident Reporting / Unusual Events reporting is provided in Annexure H.

Summary of Incidents during the quarter

On a regular basis, incidents that occurred during the quarter are summarised and reported in the format given in Annexure – I to the SPRMC for their review and necessary guidance. The Risk Manager compiles this summary using the incidents reported by various business functions and incorporates them into the Risk Register.

9.4 Policy Ownership and Revisions

Ownership of Policy and Process Documents

All policy and process documents require a defined owner who is responsible to ensure that the document is accurate and updated on a regular basis. The owner is overall responsible for the maintenance of the documents. Further, all functions and persons identified within these documents are responsible for their respective roles and responsibilities.

Detailed procedures adopted by the Company for policy ownership and revisions is provided in Annexure J

Inventory of Policy and Process Documents

The Company will maintain an inventory of policy and process documents and track timely review and approval of various policy and procedures.

10 Risk Management Culture and Training

To realise return on risk, senior management needs to ensure risk awareness is embedded into the organisation culture. This includes its consideration in key decisions, preparedness among staff to take ownership of risk within their operations and ultimately the development of integrated metrics (a common 'language') that seek to align risk and performance management across the business

All employees should have a clear understanding of their risk management responsibilities and be held accountable for their performance in that respect.

Periodic risk management training is imparted to company employees and senior management to inculcate a uniform risk management culture. Targeted trainings on specific topics are undertaken by select employees based on their role in the Risk Management Framework.

11 Review of Risk Management Policy

The Risk Manager shall have the ownership of the Risk Management Policy and shall be responsible for implementation of the policy aspects. The policy document shall be reviewed by SPRMC and approved by the Audit Committee.

The Audit Committee shall review and approve this Policy from time to time, atleast on an annual basis, to ensure it remains consistent with the Board's objectives and responsibilities.

Annexures

A. Strategic Planning and Risk Management Committee Charter

Constitution

The following shall be the members of the Committee

- Chairman and Managing Director - Chairman
- Risk Manager -Secretary
- Director Operations
- GM - Operations
- GM- CSBD
- GM-MS
- GM – Finance
- Company Secretary

Periodicity of Meetings : Quarterly

Responsibilities of the SPRMC

- Review Long Term Business Plan (LTBP) of KPL and recommend appropriate modifications/changes thereto for approval by the Board
- Set action plan priorities in line with LTBP duly incorporated in Annual Plans
- Identify projects integrated to strategic goals and objectives in line with LTBP
- Evaluate and approve projects within limits as delegated by the Board
- Monitor progress of project implementation/execution
- Administer Risk Management Framework (RMF) to identify and manage risks and monitor risk mitigation plans from time to time.
- Evaluate the adequacy of control systems including effectiveness of the internal and external audit functions and ensure that exceptions if any are timely highlighted and culminate into introduction of additional controls
- Submit a status report on the risk management processes to the Board on a half-yearly basis

- Oversee establishment of the overall risk management framework which lists type of risks which are acceptable, those which are unacceptable and a well laid out process for ongoing management of the risks
- Develop risk strategy and risk appetite statements in line with the business strategy and objectives and evaluate the same periodically
- Review and recommend risk policies for Board approval
- Ensure that staff at all levels understand their responsibility with respect to operational risk
- Report significant risk issues to the Board

B. Risk Categorisation (Part of Risk Register)

Risk Categorisation helps the Company to classify risks in terms of the broad nature of the risks and determine overall risk profile in terms of these categories.

Universe of Risk Categories		Universe of Risk Categories	
Risk Category	**Possible Identified Risks**	**Risk Category**	**Possible Identified Risks**
Strategic	Land Acquisition for future Expansion Plan Approval Business Diversity Competition Outsourcing/BOT contracts	**Operational**	Inadequate Infrastructure Industrial Relations Service Inefficiency Business Continuity Planning & Disaster Recovery Port Security Inefficient Contracting process Project Risk (Construction of new facilities)
Human Capital	Employee Skill set Maturing workforce Employee Recruitment Employee Retention Job rotation	**Financial**	Bill passing Receivables Management Economic downturn Revenue concentration Treasury & Investment Management Cost containment and budgeting Currency exposures Capital Budgeting End use of funds
Safety	Cargo Handling Fuel Handling Berth Operations Occupational Health & Safety	**Hazards**	Natural Catastrophe Environmental hazards Adverse weather Fire and Explosion
Legal/ Regulatory/ Reputation	Regulatory Reporting Non compliance Environmental non compliance Fraud & Ethics Regulatory changes Counter party contracts Dispute Resolution	**Technology**	Data privacy/Loss Data protection System failure Data backup and storage

C. Format of Risk Register

Risk Description	Risk. No.	
	Risks	Key Risks that can impact the company identified by Main business function and processes
	Causes	Causes for the risk event to occur
	Consequences	Impact or consequences if the risks were to take place
	Risk Category	Risk Categorisation to better analyze the risks. For more details on Risk categorisation, refer Annexure.
Risk Rating before Controls	Inherent Likelihood	A rating of risk likelihood on a scale of 1 to 3
	Inherent Impact	A rating of risk impact on a scale of 1 to 3
	Inherent Risk Rating	Final risk rating level before application of controls. (Scale 1-9) The rating is arrived at by multiplying likelihood and impact score.
Control Description	Current Controls	Description of current controls
	Control Assessment	(P-Poor, A- Average, G- Good)
Risk Rating after Controls	Residual Likelihood	A rating of risk likelihood, after controls and are in place, on a scale of 1 to 3
	Residual Impact	A rating of risk impact, after controls and are in place, on a scale of 1 to 3
	Residual Risk Rating	Final risk rating level after application of controls. (Scale 1-9) The rating is arrived at by multiplying likelihood and impact score.
Action Plan Details	Proposed Remedial Action for Risk Mitigation	Proposed action plans, remedial action to mitigate any residual risks.
	Action Owner	Action Owner / Department responsible to undertake the proposed actions
	Trigger	The event which will trigger to initiate the proposed remedial action. Some remedial measures which are completely absent may be initiated immediately, some other may need to be practiced on an ongoing/continuous basis.

D. Risk Assessment Parameters

IMPACT RATING PARAMETER

Impact	Comments	Minor	Moderate	Major
		1	2	3
Financial	loss (% of Gross Margin)	(1% of Gross Margin)	(2% of Gross Margin)	(5% of Gross Margin)
Reputation	Letters to local/industry press/ investor confidence/extensiveness of negativity	Series of articles or complaints in press or by customers/ business associates/ stakeholders	Extended negative local/industry coverage & short term disruption to confidence level of customers/ business associates	Extensive negative media coverage and disruption to confidence level of customers/ business associates/ stakeholders
Regulatory	Minor/penalties to business closure	Minor penalties	Major penalties	Major Censure
Business Disruption		Business disruption leading to minor business losses. One-off and/or short term disruption at the individual unit level. Middle level management required.	Business disruption leading to moderate business losses. Medium term business disruption at the business level. Business head effort required.	Business disruption leading to major business losses. Sustained period of disruption at the organisational level. Significant senior management effort required.
Safeguarding of assets and information		Communication of key information which may be publicly available. Minor fraud issues Damage or theft of Physical Assets or systems security	Communication of key information which may not be publicly available. Frauds leading to moderate losses Damage or theft of Physical Assets	Communication of highly sensitive information. Frauds leading to erosion of net worth Damage or theft of Physical Assets or systems security
Management Effort	An event which can be absorbed to event which is a disaster	An event the consequences of which can be absorbed but management is required to minimise the impact	A significant event which can be managed under normal circumstances	A disaster with potential to lead to collapse of the business

LIKELIHOOD RATING PARAMETER

Likelihood	Unlikely	Likely	Highly Likely
	0-15%	15-75%	>75%
	1	2	3
	Event could occur at sometime, although unlikely	Event will probably occur	Event is expected to occur in most circumstances

E. Risk Profile of Departments

Risk Dashboard - As of Month - Year

KPL - Summary Risk Profile													
			Risk Category As of Dec/June Year.....								Risk Category Jun/Dec Yr...		
S. N		Process/ Department	No of Risk Elements	Low 1 & 2	Med 3 &4	High 6 & 9	Gross Score	AvgScore	Average Risk Category		No of Risk Elements	Average Score	Average Risk Category
1	**Comp Secy**	**Compliance**											
2	**CSBD**	HR Admin Corp, Internal Control & RM **CSBD Total**											
3	**Finance**	**Finance**											
4	**Marine Services**	EDP Safety Services Survey & Dredging Environment **Marine Services Total**											
5	**Operation**	Building Electricals Roads & Berths Estates Projects CSR **Operations Total**											
		Overall KPL Profile									**0**		

F. Risk Calendar

Risk Management Activity	Details and Audience / Reporting To
Regularly / As needed	
Updates to Current Action Plan	Departmental Heads to execute action items identified in the Action Plan. Further, to review current Action Plan and update the Action Plan details regularly for providing periodic updates to Risk Division.
Monthly	
Updates to Current Action Plan	Risk Manager to Review current Action Plan and take updates from each Business Function and update the Action Plan column of Risk Register. In addition, update Residual Risk Rating, if required, depending on the measure of action taken, on a monthly basis.
Quarterly	
Risk Heat Maps	(1) Risk Manager to develop Departmental heat maps and reports as Risk Dashboard to SPRMC along with updated Risk Register. (2) Summary of High Risk elements in the Risk Register (residual rating 6 & 9) for review by SPRMC to be presented to the Board along with departmental Risk Dash Board
Summary of Incidents Occurred	Risk Manager compiles a summary of incidents occurred during the period and presents to the SPRMC for discussion and mitigation actions.
Project Risk Management	Risk Manager creates Consolidated Summary of all key projects (over Rs 5 crores) to be put up to the SPRMC along with key issues, current status and overall status.
Half Yearly	
Review of Risk Register	Comprehensive updates to Risk Register by Risk Manager jointly with Risk RRPs with addition/deletion of new risks/functions or rearrangement of divisions with revision of management structure. Updated Risk Register to be discussed at the SPRMC
Annually	
Review and revision to Risk Management Policy	Review of Risk Management Policy and update as necessary. Updated Risk Management Policy to be reviewed and approved by SPRMC and thereafter to be tabled to Audit Committee for Board approval.
Review of Risk Appetite	SPRMC performs discussion and review of Risk Appetite Statements. Risk Appetites shall then be placed to the Audit Committee for Board approval.

G. Summary of Project Risks and Issues

Projects	Planned Progress	Actual Progress	Key Risks and Issues	Overall Status
Project A				
Project B				
Project C				

H. Incident Reporting Procedures

Definition of an Incident

For the purpose of defining which events should be reported to senior management the following are some guidelines. However, this is not an exhaustive list and the process owners should consider the financial, operational or reputational impact of the event.

Purpose of Incident reporting

- To analyze event for ascertaining cause-effect relationship and sharing the learning from event with concerned users/ others for initiating necessary corrective steps including improvements to processes, controls and training.
- To inform facts of event to Senior Management to seek their advice/guidance for taking future course of action
- To review adequacy of risks covered and amount of insurance taken by the Company vis-à-vis actual losses suffered

Incident Reporting Process

The incident reporting process is given below.

1. Person discovering the event or loss prepares an incident report, as per defined format outlined in these procedures, to capture important information.
2. Division / Function Head review the incident report and adds necessary comments and mitigation steps taken, if initiated.
3. Mitigation and damage control steps are initiated at the earliest to protect the company and prevent further loss.
4. Incident report is sent to Risk Manager for further analysis, corrective and preventive actions and update of Risk Register.

Example of types of events that should be reported

- Breakdown of key equipment
- Financial loss due to process failure such as wrong payment to vendors contractors
- Any event that is reported in the media resulting in reputation damage
- Events involving loss &/ or theft of information
- Events resulting in disruption of routine business/operations for more than 4 hours due to reasons like natural calamities, riots, terrorist attacks, strike etc
- Internal frauds (including attempted frauds)
- Loss of human life (Company and contractors) during office hours

Incident / Unusual Event Reporting Format

Date of Reporting	Date of Detection of Event	Date of Occurrence of Event	
Business Unit		**Sub Process**	
Brief Description of the Event	Xx		
Amount Involved (Yes / No)	**Actual financial Loss**	**Recoveries**	**Net Loss**
Details of the Event: (Please add details on how the event occurred, amounts involved, losses occurred, modus operandi etc) *xxxx*			
What caused the Event: • • •			
Impact of the Event: • • • •			
Action Taken: • • •			
Reported By		**Supervisor Review**	

Please complete the above loss event reporting format and forward to Risk Management Department at the earliest. Please continue to take corrective action to prevent further losses or reputation, non compliance impact due to the event.

I. Register of Incident Reported - Format

Kamarajar Port Limited

Incident Reporting Register

Date of Incident	Date of Detection	Location	Summary of Incident (Nature of event)	Incident Description	Department	Incident Type	Financial Loss Amount, if any

J. Quarterly Report of High Risks to Board - Format

Kamarajar Port Limited						
Quarterly Report of High Risks to Board of Directors as on Dt						
S.N.	**Risk Description**	**Cause of Risk**	**Financial Loss Amount, if any**	**Remedial Action Planned/Taken**	**Action Time frame/Date**	**Action Owner**

K. Procedures for Policy Ownership and Revisions

Procedure for updates

- All documents will be reviewed and revised based on the frequency identified within that document. In case this is not specified, then the documents will be reviewed periodically as deemed by the Policy Owner
- All proposed policy updates, identified either by the Policy Owner or other business units, are summarized in the form of proposals.
- Updated policy document is circulated for review and approval by all affected business units.
- Final version is submitted to relevant approving authority
- Owner maintains the original approved policy
- Revised and approved policy document is communicated to all relevant stakeholders for immediate implementation

Procedure for policy enforcement without revisions

Minor policy amendments may be enforced without the need to revise the complete policies. However, this practice is discouraged as there is a risk that other policy users may not be aware of these interim updates.

To ensure that any such updates are properly implemented, the following procedure will be applied.

- All interim policy minor changes must be approved by the relevant approving authority, either in print or via email.
- Owner of the policy/process document must communicate this change to all relevant business units.
- The owner is required to keep track of all such policy changes.
- On a periodic basis, such interim changes should be incorporated into a formal policy/process revision.

L. Terms and Definition

Risk

Risk is often described by an event, a change in circumstances or a consequence that may occur, and whose occurrence, if it does take place, has a harmful or negative impact on the achievement of the organization's business objectives. Thus, risk is the effect of uncertainty on objectives.

Risk Management

Risk Management is the coordinated activities to direct and control an organization with regard to risk. It is the process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.

Risk Management Policy

Risk Management Policy is a statement of the overall intentions and direction of an organization related to Risk Management.

Risk Management Framework

Risk Management Framework is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving Risk Management throughout the organization.

Risk Management Plan

Risk Management Plan is a scheme or an operation plan within the Risk Management Framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk Strategy

The Risk Strategy of an organization defines its readiness towards dealing with various risks associated with the business. It describes the organization's risk appetite or tolerance levels and decision to transfer, reduce or retain the risks associated with the business.

Risk Owner

Risk Owner is a person or entity with the accountability and authority to manage risk.

Risk Assessment

Risk Assessment is defined as the overall process of risk identification, risk analysis and risk evaluation.

Risk Estimation

Risk Estimation is the process of carrying out quantitative, semi-quantitative or qualitative assessment of risk in terms of the probability of occurrence and the possible consequence.

Risk Identification

Risk Identification is a process of finding, recognizing and describing risks.

Risk Source

Risk Source is an element which alone or in combination has the intrinsic potential to give rise to risk.

Risk Tolerance / Risk Appetite

Risk Tolerance or Risk Appetite is a driver of Risk Strategy of an organization. It defines the maximum quantum of risk which the company is willing to take as determined from time to time in consonance with the Risk Strategy of the company.

Risk Description

A Risk Description is a comprehensive template covering a range of information about a particular risk that may need to be recorded in a structured manner. It is an input to the Risk Register.

Risk Register

A 'Risk Register' is a tool for recording the risks encountered at various locations and levels in a standardized format of Risk Description. It becomes a major input in formulating subsequent Risk Strategy.

Likelihood

Likelihood means the chance of something happening; whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively and described using general terms or mathematically such as a probability or a frequency over a given time Period.

Risk Profile

Risk Profile is a description of any set of risks that may relate to the whole or part of the organization or as otherwise defined.

Risk Analysis

Risk Analysis is a process to comprehend the nature of risk and to determine the level of risk. It provides the basis for Risk Evaluation and decisions about Risk Treatment and includes Risk Estimation.

Risk Criteria

Risk Criteria is a terms of reference against which the significance of a risk is evaluated. They are based on organizational objectives and external or internal context and can be derived from standards, laws, policies and other requirements.

Risk Evaluation

Risk Evaluation is a process of comparing the results of Risk Analysis with Risk Criteria to determine whether the risk and / or its magnitude is acceptable or tolerable. It assists in the decision about Risk Treatment.

Risk Treatment

Risk Treatment is a process to modify a Risk. It that deals with negative consequences is also referred to as ‘Risk Mitigation’, ‘Risk Elimination’, ‘Risk Prevention’ and ‘Risk Reduction’. It can create new risks or modify existing Risks.

Control

Control is a measure of modifying risk and includes any process, policy, device, practice or other actions which modify risk. It may not always exert the intended or assumed modifying effect.

Residual Risk

Residual Risk is a risk remaining after Risk Treatment. It can contain unidentified risk and also be known as ‘Retained Risk’.

Terms and definitions not covered hereinabove will have the meaning as indicated under ISO 31000 : 2009.