ALLCARGO TERMINALS LIMITED

ENTERPRISE RISK MANAGEMENT (ERM) POLICY

Contents

1. BACKGROUND

Allcargo Terminals Limited was established with a vision to tap into the immense opportunities in the cargo terminals vertical owing to the increasing EXIM trade opportunity in India. The company operates on an asset light business model and its core business comprises of Container Freight Stations (CFS) and Inland Container Depots (ICD). As an extension of the port infrastructure, CFSs and ICDs also offer services like Customs inspection/clearance, Stuffing/Destuffing, Weighment and storage, among others. Allcargo Terminals Limited is one of the largest CFS operators in India with a combined installed capacity of over one million square feet. Formerly a division of Allcargo Logistics Limited, it started CFS operations in 2003 with its first CFS at JNPT in Mumbai. Thereafter, the journey of growth continued with offering one of India's widest CFS-ICD networks.

2. REGULATORY REQUIREMENT

As per SEBI (Listing Obligation and Disclosure Requirements) Regulations 2015, every listed company is required to develop and implement Enterprise Risk Management Policy for the Company. The Board of Directors and the Risk Management Committee is responsible to ensure that the Company has a robust Enterprise Risk management policy and monitor its effectiveness on a periodic basis.

3. SCOPE

Enterprise Risk Management Policy ("ERM Policy") establishes the philosophy of the Company, towards risk identification, analysis and evaluation, prioritization of risks, development of risk mitigation plans, monitoring and reporting on the risk environment of the Company. This policy is applicable to all the functions and departments of the Company including its subsidiaries.

4. OBJECTIVE

The purpose of the Enterprise Risk Management Policy is to institutionalise a formal risk management function and framework in the Company. The objective of this policy is to manage the risks involved in all activities of the Company to maximize opportunities and minimize adversity. This policy is intended to assist in decision making processes that will minimize potential losses, apprise the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives.
The key objectives of this policy are:

1) Safeguard the Company property, interests, and interest of all stakeholders.
2) Lay down a framework for identification, measurement, evaluation, mitigation and reporting of various risks.

3) Evolve the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects, which the business and operations of the Company are exposed to.
4) Balance between the cost of managing risk and the anticipated benefits.
5) To create awareness among the employees to assess risks on a continuous basis and develop risk mitigation plans in the interest of the Company.
6) Provide a system for setting of priorities when there are competing demands on limited resources.

5. GOVERNANCE STRUCTURE

The company has established three levels of risk management responsibilities in its governance structure.

6. RISK GOVERNANCE

Board of Directors:
The Board shall be responsible for defining the enterprise risk management strategy and objectives, overseeing the implementation of the enterprise risk management process and setting the tone and culture towards effective enterprise risk management. The board shall define the enterprise risk management policy and critically review the risk governance and monitoring mechanism.

The Company shall lay down procedures to inform members of Board of Directors about risk assessment and minimization procedures.

The Board of Directors shall be responsible for:
1) Framing, implementing and monitoring the risk management plan for the Company;
2) Reviewing and guiding on the Enterprise Risk Management Policy;
3) Ensuring that appropriate systems of control are in place, in particular, systems for risk management;
4) Report of Board of Directors shall include a statement indicating development and implementation of enterprise risk management policy for the Company.

Risk Management Committee (RMC):

Risk Management Committee (RMC or the Committee) is chaired by an Independent Director and it shall meet at least twice in a year or at such intervals as may be deemed fit. Quorum for the RMC meeting shall consist of 2 members out of which 1 from Board members and 1 from other members.

RMC shall have the following set of responsibilities:

1) To formulate a detailed Enterprise risk management policy including the following and recommend the board for its approval,
   a. A framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, ESG related risks), information, cyber security risks or any other risk as may be determined by the Committee,
   b. Measures for risk mitigation including systems and processes for internal control of identified risks.
   c. Business continuity plan
2) To monitor and oversee implementation of the enterprise risk management policy, including evaluating the adequacy of risk management systems;
3) To periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity;
4) To ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the company.
5) To keep the Board of Directors informed about the nature and content of its discussions, recommendations and actions to be taken;
6) To ensure risk assessment and mitigation procedures are implemented.
7) To review the appointment, removal and terms of remuneration of the Chief Risk Officer.
8) RMC shall have access to any internal information necessary to fulfil its oversight role. It shall also have authority to obtain advice and assistance from internal or external legal, accounting or other advisors;
9) RMC shall have powers to seek information from any employee, obtain external legal or other professional advice and secure attendance of outsiders with relevant expertise, as it deems necessary;
10) To ensure that it is apprised of the most significant risks along with the action management is taking and how it is ensuring effective ERM;
11) To review risk disclosure statements in any public documents or disclosures;
12) To be aware and concur with the Company's risk appetite including risk levels, if any, set for financial and operational risks;
13) To ensure that the Company is taking appropriate measures to achieve prudent balance between risk and reward in both ongoing and new business activities;
14) To review the Company's portfolio of risks and consider it against the Company's Risk Appetite;
15) Being apprised of significant risk exposures of the Company and whether Management is responding appropriately to them;
16) Perform other activities related to this Policy as requested by the Board of Directors or to address issues related to any significant subject within its term of reference.

Chief Risk Officer:
The Risk Officer shall ensure risk management processes as defined in this policy are executed and coordinate the effort of various functions to deliver consolidated view to the Board and the RMC.

The Risk Officer would also be responsible for conducting internal risk review meetings, maintaining risk registers and enterprise risk management policy, and suggesting best practices for strengthening the risk management process. Risk register is maintained basis approved parameters for risk evaluation and the same are reviewed periodically for validation.

Functional & Departmental Heads:
The final ownership of risk identification, monitoring and mitigation shall rest with the respective functional heads. The function heads of various business units shall accept the risk of their respective areas and own the risk management plan of their unit.
The risk owner shall drive and monitor the progress of the mitigation strategies. Every business function/department will depute a manager not below a manager level as the "Risk Champion" to ensure compliance to this policy and ground level implementation of the mitigation action plans. The risk champions shall also be responsible for reporting the status of mitigation plan to the Chief Risk Officer. For cross-functional risk, a cross-functional team with clear demarcated roles and responsibilities shall be formed to drive implementation of mitigation action plans and review risk status periodically.

7. Composition of Risk Management Committee (RMC):

The Risk Committee constitution is as follows:

Sr No	Name of the Member	Position in the Committee	Category
1.	Mrs Radha Ahluwalia	Chairperson	Independent Director
2.	Mr Vaishnavkiran Shetty	Member	Non-Executive Non-Independent Director
3.	Mr Prafulla Chhajed	Member	Independent Director
4.	Mr Ashish Chandna	Member	Chief Executive Officer

8. ENTERPRISE RISK MANAGEMENT PROCESS

In order to manage in a systematic manner, the Company has defined Enterprise Risk Management process that is based on industry standards and encompassing all risks that the organization is facing internally or externally under different categories such as strategic, operational, sectoral, legal and compliance risks including ESG and Cyber security risks.

The process is designed in alignment with the basic elements of Enterprise Risk Management process steps and components put forth as per ISO 31000.

The process prescribes detailed procedures and guidelines for contextualization of risks by linking it to strategic objectives, identification, assessment, mitigation, any internal controls, communication, monitoring and governance. Appropriate risk indicators are used to identify risks proactively. The framework takes cognizance of risks faced by key stakeholders and the multiplied impact of the same on the organization which may impact business continuity while framing risk responses.

The Company maintains procedures to provide the systematic view of the risk faced by the Company in the course of its business activities. This will require the Company to:

1) **Establish a context:** Criteria against which risk or opportunity will be evaluated should be established and the structure of the risk analysis defined.
   *The purpose of establishing the context in the assessment is to set the stage for risk and opportunity identification. Since "risk" (opportunity) is defined as "any issue (negative or positive) that may impact an organization's ability to achieve its objectives," defining the organization's objectives is a prerequisite to identifying risks and opportunities***.**
2) **Identify Risks:** This is the identification of what, why and how events arise as the basis for further analysis.
3) **Analyse Risks:** This is the determination of existing controls and the analysis of risks in terms of the consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequence and likelihood are combined to produce a risk score.
4) **Evaluate Risks:** This is a comparison of estimated risk levels against pre-established criteria. This enables risks to be ranked and prioritized.
5) **Mitigate Risks:** For higher priority risks, the Company is required to develop and implement specific risk management plans including funding considerations. Lower priority risks may be accepted and monitored regularly.
6) **Monitor:** This is for the oversight and review of the risk management system and any changes that might affect it. Monitoring and reviewing occurs concurrently throughout the risk management process.
7) **Review and Report:** Appropriate communication and consultation with internal and external stakeholders should occur at each stage of the enterprise risk management process.

9. CLASSIFICATION OF RISKS:

Risks Identification & Classification

This would envisage identification of the potential list of events/ perils/ risks/ factors that could have an adverse impact on the achievement of business objectives. Risks can be identified under the following broad categories.

1. INTERNAL RISKS	
Risks associated with activities affecting the business operations in a short to long term basis. Project viability, process risk, technology obsolescence/ changes, development of alternative services.	
Strategic Risk	Risks associated with an organization's inability to formulate and/or execute a successful business strategy largely having to do with the future growth plans of the Company. Emerging businesses, Mergers & Acquisitions, capital expenditure for capacity expansion and other purposes are normal strategic risks faced by the Company.
Operational Risk	Process bottlenecks, non-adherence to process parameters/ pre-defined rules. Risks in multi-level and multi-location business operating model are driven by local business environment and covered under this category.
Finance Risk	Financial Risks includes but is not limited to risks associated with liquidity, credit, currency fluctuation, changes in interest rates, changes in taxation policies, financial leverage risk, expenditure risk.
Human Resource Risk & Human Rights Risk	Non-availability of competent manpower, high attrition & absenteeism ratio, Brain-drain or attrition of critical talent, retention challenges and increase in training cost, succession planning etc. Nonadherence to basic norms for Human Rights of equality, inclusivity, safety, child labour/ POSH compliances.
Legal / Regulatory Risk	Legal risk is the risk in which the Company is exposed to any legal action resulting from its operations including Contract Risks and Contractual Liability.
Information Technology / Cyber Security Risk	Risk associated with information technology and cyber security like preventing of hacking incidents, losing of sensitive, confidential data etc. New and emerging technologies bring unprecedented threats to internet connected devices, including vehicles. The loss of sensitive and personal data or a breach in any safeguards aimed at protecting the information related to cyber security could lead to significant legal action combined with the imposition of regulatory and associated fines.

Health & Safety Risk	Facilities at various locations and labour-intensive nature of work comprises health risks for the workforce due to reasons like machinery breakdown, human negligence, among others
ESG Risk	Environmental risks that may arise from operations due to the impact of our services shall be considered while evaluating risks. Risks may be related to climate change, waste management, water management, among others. Governance risks can include risks from non-compliance and changes in regulatory norms and policies which may negatively impact the Company. Risks related to the structure, policies, procedures and authorities in which the key directions and decisions of the Company are overseen.

2. EXTERNAL RISKS	
Market Environment Risk	Risks associated with the environment in which the client operates or external factors beyond the company's control e.g. competition, Risks arising out of changes/ actions of customer/vendor or other business counterparts.
Legal / Regulatory Risk	Potential risk arising changes in laws and regulations, rules, government policies, tax regulations, technical standards and trade policies.
ESG Risk	Environmental risks that may arise from natural calamities such as floods, earthquakes, cyclones and storms. Societal risks such as conflict in community, relationship with stakeholders and social issues shall be considered while evaluating risks.
Geo-Political Risk	Changes in the political environment, regulation/ deregulation due to changes in political environment.
Reputation Risk	Brand impairment, Statutory liabilities.

10. Evaluation and Prioritization of Risks

Risks classified as above will assigned risk levels against pre-established criteria defined below. This will enable risks to be ranked and prioritized. The risks can be evaluated by plotting them on the Risk Map based on the risk score.

Risk Likelihood Measurement

Likelihood Measurement Unit	Probability (%)	Numeric Value
Rare	<20%	1
Unlikely	21%-40%	2
Possible	41%-60%	3
Likely	61%-80%	4
Almost Certain	>80%	5

Risk Impact Measurement:

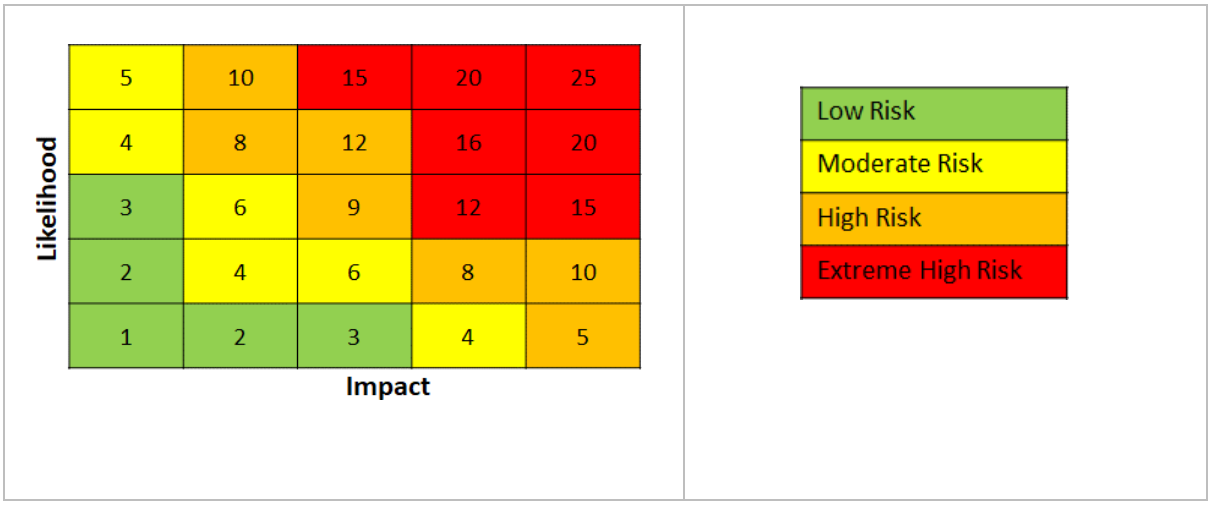
Impact Measurement Unit	Risk Description- Non transaction Risks	Numeric Value	% of PBT
Insignificant	Impact is insignificant	1	<0.5%
Low	A low impact event on the organizational objectives	2	0.5% to <2%
Moderate	Event will have impact on organizational objectives.	3	2% to <3.5%
Significant	Impact is high and can affect organizational objectives	4	3.5% to <5%
Critical	Impact is extremely high and can severely affect organizational objectives.	5	5% and above

Certain risks, which cannot be quantified in monetary terms and as such not possible to rank them. In such cases, the consequences of the risk need to be evaluated based on below mentioned parameters:

- Impact on fatality or irreversible disability/impairment to human life;
- Impact on the environment;
- Impact on the Brand Equity including public litigation.

Risk Levels

Each risk statement will be assessed for impact and likelihood on the scale of measurement tabulated above. Risk score will be calculated as product of likelihood and impact. Based on the score and assessment of non-financial impact, the risks will be classified in to four categories such as Extreme High Risk (Catastrophic), High Risk (Critical), Moderate Risk (Cautionary), and Low Risk (Acceptable). Assignment of Risk levels will be weighted based on the impact inherent in the Risk Score i.e. same risk score with higher impact component will be assigned a higher risk level based on the magnitude of the impact score.



Retention of Documents

Risk Management Plans, risk matrix or risk mitigation plans shall be retained by the Company for a minimum period of five years or as per regulatory requirements.

11. Policy Review:

The policy will be reviewed once in two years for modification based on change in business environment and practices.

Version/Date of Committee/Board Approval	Effective Date	Description of changes	Next Review
1.0	May 17, 2024	Adopted and approved by Board of Directors in their meeting held on May 17, 2024	-

****