RISK MANAGEMENT POLICY

Under Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

KRISHNA BUILDSPACE LIMITED
(Formerly known as Krishna Buildspace Private Limited)
CIN: U45200GJ2013PLC076590
Registered Office: 510-Zion Prime, Thaltej Shilaj Road, Before Shilaj Railway Crossing,Thaltej, Ahmedabad, Gujarat- 380059
Telephone No.: 07935188376 | Email: accounts@krishna.build
Website: www.krishna.build

RISK MANAGEMENT POLICY

1. INTRODUCTION

The Companies Act, 2013 emphasizes the requirement of Risk Management Policy for the Company. Section 134(3)(n) of the Companies Act, 2013 requires that the report by the Board of Directors laid at the general meeting shall include a statement on the 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 shall be included in the Board's Report.

The Audit Committee is required to evaluate the internal financial controls and risk management systems of the Company and the Independent Directors shall satisfy themselves that the systems of risk management are robust and defensible. Section 177(4)(vii) of the Companies Act, 2013 provides that Audit Committee shall evaluate the internal financial controls and risk management systems of the company.

Regulation 17(9) (a) of SEBI (Listing Obligation and Disclosure Requirements) Regulations, 2015, inter alia, mandates laying down the procedures for risk assessment and minimization. Further Regulation 17(9)(b) of the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, provides the Board of Directors shall be responsible for framing, implementing and monitoring the risk management plan for the company.

Regulations 21(4) further provides that the board of directors shall define the role and responsibility of the Risk Management Committee and may delegate monitoring and reviewing of the risk management plan to the committee and such other functions as it may deem fit. Such function shall specifically cover cyber security. It further states that role and responsibilities of the Risk Management Committee shall mandatorily include the performance of functions specified in Part D of Schedule II.

The Board of Directors (**"the Board"**) of Krishna Buildspace Limited(**"the Company"**) has adopted the following policy and the Board may amend this policy from time to time. In case of any subsequent amendments to the Regulations which makes any of the provisions in the Policy inconsistent, the provisions of the Regulations shall prevail.

2. OBJECTIVE OF POLICY

The objective of this policy includes the following:

- Develop a risk culture that encourages all employees to identify risks, associated opportunities/gains and respond to them with effective actions
- Develop both proactive and reactive mechanism for risk management
- Identify and manage existing/new risks in a planned and coordinated manner by Risk Register and Risk Control Matrix
- Develop an incident response management framework to manage the risks that may materialize.

3. DEFINITIONS

"Company" means Krishna Buildspace Limited.

"Risk" means a probability or threat of damage, injury, liability, loss, or any other negative occurrence that may be caused by internal or external vulnerabilities; that may or may not be avoidable by pre-emptive action.

"Risk Management" is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

"**Senior Management**" means officers/personnel of the Company who are members of its core management team comprising all members of management one level below the Managing Director or Whole Time Director or Manager, including the functional heads and shall specifically include company secretary and Chief Financial officer.

"Risk Management Committee" means the Committee formed by the Board as under Regulation 21 of the

Listing Regulations.

Words and expressions used and not defined in this Policy shall have the meaning ascribed to them in the SEBI Listing Regulations, the Securities and Exchange Board of India Act, 1992, as amended, the Securities Contracts (Regulation) Act, 1956, as amended, the Depositories Act, 1996, as amended, or the Companies Act and rules and regulations made thereunder.

4. RISK MANAGEMENT POLICY & FRAMEWORK

Risk is the potential for failure or loss of value or the missed opportunity for value creation / strategic competitive advantage resulting from either a certain action or a certain inaction.

Controlling risk is essential in any business by having processes to ensure safeguarding of assets and compliance with appropriate regulatory frameworks. However, risks may also have to be taken consciously to explore untapped business opportunities in line with the corporate strategy to optimize maximum potential stakeholder's value and to improve their confidence.

Classification of Risks:

A. Financial / Operational / Preventable / Compliance risks:

These are internal risks, arising from within the organization that are controllable and need to be eliminated or avoided. The examples are:

- Governance, organizational structure, roles and accountabilities;
- Policies, objectives and the strategies that are in place to achieve them;
- Contractual compliances;
- Operational efficiency;
- Credit and liquidity risk;
- Human resource management;
- Hurdles in optimum use of resources;
- Culture and values;
- Suppliers/Raw Material Risk;
- Customers Risk;
- Technological Risk;
- Physical risk – that is risk of damage/breakdown to the assets of the company.

B. External risks

External risks come up due to economic events that arise from outside of an institution's control. It arises from the external events that cannot be controlled by any an institution, cannot be forecasted with reliability, are normally beyond its control, and it is therefore difficult to reduce the associated risks. The examplesare :

- Statutory/ regulatory changes/ changes in government policies;
- Market conditions/ trends;
- Economic environment;
- Political Environment;
- Fluctuations in trading activities;
- Foreign Exchange Rate Risk;
- Factors beyond the company's control (including act of God, epidemic, pandemic, war, etc.) which significantly reduces demand for its business and/or affects its operations.

C. Disruptive risks:

These are the anticipated or unanticipated events which may result in disruption of the operations of Company or existence of its current business model and Innovations to business models that disrupt the existing paradigm

D. Strategic Risks:

Risks taken on consciously linked to strategic choices to earn a higher return.

The aggregate level and types of risk the Company is willing to assume within its risk capacity to achieve its strategic objectives and business plan shall be as per its risk appetite. The Risk Management process involves the following phases:

- Risk identification
- Risk evaluation and assessment
- Risk mitigation

4.1 Risk Identification

This involves continuous identification of events that may have a negative impact on the Company's ability to achieve goals. The company has adopted a robust risk identification process keeping in view the key activities/ focused areas of company's business for the purpose of risk assessment. Identification of risks, risk events and their relationship are based on the basis of discussion with the senior management and analysis of related data/ reports, previous internal audit reports, past occurrences of such events etc. The identification of risk by the company is broadly based on the following internal and external risk factors:

The risks can be broadly identified/ categorized into one or more following categories; however, the risk management committee may revise such categories:

Category of Risk	Examples
Financial Risks	· Financial misstatements/ improper accounting or financial reporting. · Unavailability of funding and cash flow; · Change in credit limit affecting availability of funds; · Market conditions on lending / borrowing of funds; · Loan repayment schedules not adhered; · Changes in the applicable laws and environment related to funding, investment norms, including raising of funds from international market;
Operational Risks	· Business disruption; · Delay in implementation of project/ plan; · Inefficient use of resources/increased product/ service cost; · Physical property/damage/disruption; · Accidents / force majeure events, change in management, etc. · Limited availability of manpower and resources;
Sectoral Risks	· Product development and engineering activities; · Limited number of customers including government customers; · Third Party suppliers for our key components, materials; · Inability to implement business strategies; · Cyclical demand and vulnerable to economic downturn; · Competition with certain key players in the industry; · Regulatory approvals and licenses for business; · Changes in the energy industry and governmental energy policies.
Sustainability (ESG Related) Risks	· Non-compliance of environmental, social and governance related laws; · Adaptability to changes in the applicable laws including those related to ESG norms such as labour laws; · Strained employee relations due to any reason, strikes, lock-outs, accidents, salary disputes etc.
Information Risks	· Leakage of key/sensitive non-public information; · Rumors in the market and / or related trading in the securities of the Company;

	· Adverse national media or public or national government attention · Data Privacy challenges;
Cyber Security Risks	· Disruption of IT operations; · Server issues; · Phishing, data leakage, hacking, insider threats, etc.
Strategic Risks	· Reduction in business vitality (due to change in business strategy, customer spending patterns, changing technology, etc.); · Loss of intellectual property and/or trade secrets; · Competition for talent; · Negative impact to reputation/loss of trust mark.
Compliance Risks	· Violation of laws or regulations governing areas including but not limited to:
	· Environmental;
	· Employee health & safety;
	· Labour laws;
	· Product quality/safety issues ;
	· Local tax and statutory laws.
	· Prosecution, fines, investigations, inquiries; litigation including class actions.

4.2 Risk Analysis

Risk analysis involves:

- consideration of the causes and sources of risk;
- the trigger events that would lead to the occurrence of the risks;
- the positive and negative consequences of the risk;
- the likelihood that those consequences can occur.

Factors that affect consequences and likelihood should be identified. Risk is analyzed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

4.3 Risk Assessment

Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. The Company has assigned quantifiable values to each risk element based on the "impact" and "likelihood" of the occurrence of the risk on a scale of 1 to 4 as follows.

Impact	Risk Level	Likelihood
Minor	1	Low
Moderate	2	Medium
High	3	High
Critical	4	Critical

4.4 Risk Mitigation

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Once implemented, treatments provide or modify the controls.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of that treatment.

Based on the Risk level, the company should formulate its Risk Management Strategy. The strategy will broadly entail choosing among the various options for risk mitigation for each identified risk. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Following framework shall be used for risk treatment:

1. Risk Avoidance (eliminate, withdraw from or not become involved)
   Risk avoidance implies not to start or continue with the activity that gives rise to the risk.

2. Risk Reduction (optimize -mitigate)
   Risk reduction or "optimization" involves reducing the severity of the loss or the likelihood of the loss from occurring. Acknowledging that risks can be positive or negative, optimizing risks means finding a balance between negative risk and the benefit of the operation or activity; and between risk reduction and effort applied.

3. Risk Sharing (transfer - outsource or insure)
   Sharing, with another party, the burden of loss or the benefit of gain, from a risk.

4. Risk Retention (accept and budget)
   Involves accepting the loss, or benefit of gain, from a risk when it occurs. Risk retention is available strategy for risks where the cost of insuring against the risk would be greater over time than the total losses sustained. All risks that are not avoided or transferred are retained by default. This includes risks that are so large or catastrophic that they either cannot be insured against or the premiums would be infeasible. This may also be acceptable if the chance of a very large loss is small or if the cost to insure for greater coverage amounts is so great it would hinder the goals of the organization too much.

4.5 Risk Reporting

Periodically, key risks are reported to the Board or risk management committee with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk-based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carries out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

On regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the CFO, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

5. RISK MANAGEMENT TOOLS

The Management shall adopt a comprehensive set of Risk Management Tools consisting of Risk Register, Risk Control Matrix and Internal Financial Control Audit.

5.1 Risk register is a repository of risks identified by the management w.r.t the entity and its operations, which may be financial and/or operational. The Risk Register shall be made comprehensively by all functional Heads relating to their respective areas and be duly reviewed by CEO and CFO before submission to Audit

Committee and/ or Risk Committee.

Risk Register- Salient Features:

- Collates risk information to enable effective sharing and communication of that information.
- Focuses attention on the key risks and therefore drives action.
- Is linked to the capital requirements of the organization
- Assists in developing a portfolio view of risk.
- Forms the core of an organization's risk knowledge database and is the basis for risk analysis and reporting.
- Facilitates monitoring and review.
- Evidences a systematic and comprehensive approach to risk identification.
- Is subject to regular review and update.

The Risk Register: A risk register typically captures:

- A description of the risk – including causes and influencing factors, both internal and external.
- The classification of risk category.
- Probability of occurrence.
- Risk ownership.
- Risk Priority classification.

5.2 Risk control matrix is a repository of controls placed by the management to implement measures to mitigate the risks, identified in the risk register.

5.3 IFC Audit, from a Companies Act point of view, is a test of controls implemented by the management to mitigate the risks, i.e., to test the design and operating effectiveness of these controls.

6. ROLES ANDRESPONSIBILITIES

The Risk Management Committee shall be responsible for framing, implementing and monitoring the risk management policy for the company. The Audit Committee shall review risk management systems on 3 year and ensure that adequate risk management systems are in place.

7. REVIEW OF THISPOLICY

This Policy shall be reviewed by the Risk Management Committee periodically, at least once in 3 years, including by considering the changing industry dynamics and evolving complexity.

8. BUSINESS CONTINUITY PLAN

Business continuity plan refers to maintaining business functions or quickly resuming them in the event of a major disruption, in other words, a disaster management plan. The Company shall formulate a business continuity plan as may be required for protecting the interest of the Company in the event of happening/ occurrence of any unforeseen events that may affect the business of the Company.

Such business continuity plan may vary from time to time depending on Company’s need and the risk management strategy being adopted by the company at such time. The business continuity plan may, among other things, focus on protecting the assets and personnel of the Company in the event of a disaster event which affects day to day operations of the company’s business. The business continuity plan may be reviewed and amended by the RMC from time to time, as the committee may deem fit.