KILBURN ENGINEERING LIMITED

RISK MANAGEMENT POLICY

The revised policy has been approved by the Board of Directors at their meeting held on 26th May, 2026

1. Purpose

This Risk Management Policy has been formulated to provide a structured and systematic approach for identifying, evaluating, mitigating, monitoring, and reporting risks that may impact the Company's business operations, objectives, stakeholders, reputation, compliance obligations, and financial performance. The Policy aims to support informed decision-making and promote a proactive risk management culture across the organization.

The objective of this Policy is to strengthen and enhance the Company's risk management framework by ensuring that potential risks are identified and addressed in a timely, consistent, and effective manner. The Policy also seeks to facilitate sustainable business operations, safeguard the interests of stakeholders, and support the achievement of the Company's strategic and operational goals.

2. Approach

The Company recognizes that in an evolving and competitive business environment, effective risk management plays a critical role in achieving sustainable growth, operational excellence, and long-term value creation.

The Company's risk management philosophy is founded on the principle of promoting business growth and competitiveness through informed decision-making, responsible risk-taking, and continuous risk mitigation.

The Company believes that risks are an inherent part of business operations and strategic initiatives. Accordingly, the risk management framework shall seek to create a balanced and transparent environment where risks are identified, evaluated, monitored, and managed in a structured manner to support business objectives and profitability.

The risk management approach of the Company aims to strengthen operational efficiency, business continuity, innovation, technology adoption, product and service quality, customer satisfaction, and organizational resilience. The framework is intended to foster a proactive risk-aware culture across the organization, where prudent and necessary business risks are evaluated constructively rather than avoided unnecessarily.

The Policy is designed to remain flexible and dynamic so that it can adapt to changing business conditions, operational requirements, regulatory developments, and emerging market trends. Material risks identified by the management, along with mitigation measures and action plans, shall be periodically reviewed by the Board of Directors.

The Company shall also continuously monitor potential external developments including economic conditions, regulatory changes, technological advancements, industry trends, geopolitical developments, and other relevant factors that may impact the Company's business operations or strategic objectives.

Risk management responsibilities shall be integrated across all levels of the organization, with appropriate allocation of responsibilities, resources, and reporting mechanisms to ensure effective implementation and continuous improvement of the risk management framework.

3. Scope

a) This Policy shall apply to all business activities, functions, projects, proposals, and operations of the Company.

b) All significant proposals and business decisions shall include appropriate risk assessment and mitigation measures, considering their financial, operational, strategic, and reputational impact.

c) Risks arising from contracts, commercial arrangements, and negotiations shall be identified and addressed by the concerned departments.

d) The scope of this Policy includes risks relating to:
- legal and regulatory compliance;
- operations and business processes;
- finance and investments;
- information technology and cybersecurity;
- fraud, misconduct, and corruption;
- environmental, social, and governance matters;
- reputation and external business environment.

e) The Policy shall be implemented across all levels of the organization through appropriate monitoring, reporting, and review mechanisms.

4. Responsibility

a) The management and functional heads shall be responsible for establishing and implementing effective processes for identification, assessment, mitigation, monitoring, and review of risks across their respective functions and operations.

b) The concerned departments and officials shall continuously monitor internal and external risk factors, including economic, regulatory, operational, technological, market, and business environment-related risks.

c) Functional heads and senior management shall ensure that employees involved in planning, operational activities, contracting, negotiations, and decision-making processes are adequately informed and trained on the Company's risk management framework and procedures.

d) Appropriate mitigation plans shall be developed for identified risks, with clearly defined responsibilities, timelines, and monitoring mechanisms.

e) The status of risk mitigation measures shall be periodically reviewed by the management to ensure timely implementation and effective closure of identified risks.

f) The concerned officials and departments shall also ensure compliance with applicable internal policies, legal requirements, ethical standards, and governance frameworks relating to risk management, fraud prevention, and misconduct control.

5. Framework

The Company shall establish an appropriate framework for identification, assessment, analysis, mitigation, monitoring, and reporting of risks across all business functions and operational areas.

The risk management framework shall be based on structured processes, internal controls, operational reviews, compliance mechanisms, and management oversight systems, as may be considered appropriate by the Company.

The framework shall support proactive identification of potential risks and facilitate timely implementation of mitigation measures.

6. Key Definitions and Explanation

Risk: "Risk" refers to any internal or external event, condition, circumstance, or uncertainty that may adversely impact the Company's business objectives, operations, financial performance, reputation, compliance status, or strategic initiatives.

Risks may arise from operational activities, strategic decisions, market conditions, regulatory changes, technological developments, human errors, or unforeseen external events.

Certain risks may also arise from unintended consequences of business decisions or changing business environments.

Risk Assessment: Risk assessment involves evaluation of the likelihood and potential impact of identified risks based on available information, management judgment, operational experience, and business considerations. Risks may be assessed through qualitative or quantitative methods, depending upon the nature, complexity, and significance of the risk involved.

7. Categories of Risks

Risks shall be categorized to enable effective identification, assessment, monitoring, mitigation, and management of risks across the organization. The Company recognizes that certain risks are unavoidable and may be necessary for business growth, innovation, and long-term sustainability.

a. Preventable Risks

Preventable risks are internal risks that are largely controllable in nature. These risks may arise from:

- process failures;
- system inadequacies;
- regulatory non-compliance;
- quality lapses;
- human errors;
- fraud or misconduct;
- inadequate controls or documentation.

Preventable risks shall be managed through:\n - strong internal controls;\n - compliance and audit mechanisms;\n - quality management systems;\n - cybersecurity controls;\n - employee training and awareness programs;\n - ethical and governance frameworks.\n\n- The Company shall endeavor to minimize preventable risks, particularly in compliance-sensitive and operationally critical areas.\n\n---\n\n###

b. Strategic Risks

Strategic risks arise from business decisions and initiatives undertaken for growth, competitiveness, innovation, and long-term value creation. These risks may arise from:

- business expansion;
- investments and capital allocation;
- new products or services;
- technology adoption;
- strategic partnerships;

- market and competitive developments.
- Strategic risks shall be managed through:
- detailed risk assessments;
- financial and commercial evaluations;
- management and Board oversight;
- periodic performance reviews;
- diversification and contingency planning.

The Company may accept strategic risks within approved business and operational limits to support sustainable growth and competitiveness.

c. External Risks

External risks arise from factors beyond the Company's direct control. These risks may include:

- regulatory and policy changes;
- economic and market conditions;
- geopolitical developments;
- supply chain disruptions;
- technological changes;
- natural disasters and external events.

External risks shall be managed through continuous monitoring of external developments; business continuity planning; supplier diversification; contingency measures; resilience and preparedness initiatives.

The Company shall focus on minimizing the impact of external risks and strengthening organizational resilience against such disruptions.

8. Suggested Risk Mitigation Measures

The Company may identify and evaluate significant risks that could adversely impact its operations, financial performance, reputation, business continuity, or strategic objectives. Appropriate mitigation measures may be developed and implemented to minimize the likelihood and impact of such risks.

a) Product and Operational Risks

- Risks relating to product performance, quality standards, technology gaps, process inefficiencies, or operational failures may be periodically reviewed by the concerned departments.
- Adequate supervision, quality control mechanisms, internal monitoring systems, and use of technology-enabled controls may be adopted to strengthen operational efficiency.
- Contractual risks, including delays, inadequate transfer of technology, or ambiguities in agreements, may be reviewed through appropriate legal, technical, and commercial evaluation processes.
- The Company may establish suitable review and escalation mechanisms for timely identification and mitigation of operational risks.

b) Product Delivery and Supply Chain Risks

- Risks affecting timely delivery of products or services, including project delays, vendor dependency, inventory issues, and outsourcing risks, may be regularly monitored.
- Appropriate mitigation plans may be developed to address risks relating to supply chain disruptions, certification delays, procurement issues, and force majeure events.
- Vendor assessment and periodic review mechanisms may be implemented to ensure continuity and reliability in supply and delivery processes.
- The Company may formulate suitable contingency and business continuity measures to minimize disruptions in operations.

c) Financial Risks

- Financial risks such as cost overruns, budgetary deviations, liquidity concerns, cash flow constraints, and inefficient utilization of resources may be monitored through appropriate financial control systems.
- Periodic financial reviews, audits, budgeting mechanisms, and management reporting systems may be implemented to strengthen financial governance.
- Strategic and financial planning exercises, including SWOT analysis and forecasting, may be undertaken to identify emerging risks and develop mitigation strategies.
- Risks arising from investments, development projects, or capital allocation decisions may be assessed periodically by the concerned management teams.

d) Stakeholder and Regulatory Risks

- Risks arising from changes in government policies, regulatory requirements, contractual obligations, or stakeholder expectations may be evaluated on a continuous basis.
- The Company may establish processes to assess and mitigate risks transferred through business partners, vendors, customers, or external agencies.
- Appropriate reporting and monitoring mechanisms may be adopted for regulatory and compliance-related matters.

e) Human Resource Risks

- Risks relating to talent acquisition, retention, succession planning, employee engagement, and knowledge management may be reviewed periodically.
- The Company may implement suitable training, development, welfare, and retention initiatives to address workforce-related risks.
- Human resource policies may be strengthened to ensure continuity of critical skills and competencies within the organization.

f) Compliance and Legal Risks

- Legal and statutory compliance risks may be monitored through periodic reviews by the concerned departments and compliance teams.
- Appropriate legal advisory, documentation, compliance tracking, and internal control mechanisms may be implemented to minimize legal exposure.
- The Company may establish procedures for timely identification and resolution of litigation, contractual disputes, and regulatory non-compliances.

g) Integrity and Ethical Risks

- Risks relating to fraud, corruption, unethical conduct, or misconduct may be addressed through vigilance mechanisms, internal controls, whistleblower processes, and code of conduct policies.
- Appropriate preventive and corrective measures may be implemented to strengthen transparency, accountability, and ethical business practices.
- Periodic monitoring and reporting of integrity-related matters may be undertaken by the concerned authorities.

h) ESG and Sustainability Risks

- Environmental, Social, and Governance (ESG) risks may be assessed and managed in line with applicable regulatory requirements and sustainability objectives.
- The Company may undertake appropriate initiatives relating to environmental protection, employee welfare, social responsibility, and governance standards.
- ESG-related disclosures and compliance requirements may be reviewed periodically.

i) Cyber Security and Information Technology Risks

- Cyber security risks, data protection risks, and information security vulnerabilities may be managed through appropriate IT security frameworks and monitoring systems.
- The Company may implement access controls, data protection measures, cyber security protocols, and incident response mechanisms to safeguard its systems and information assets.
- Periodic assessment and review of cyber security preparedness may be carried out.

j) Business Continuity Risks

- The Company may establish Business Continuity Plans (BCP) and disaster recovery mechanisms to ensure continuity of critical business operations during unforeseen events.
- Periodic testing, review, and updating of continuity plans may be undertaken to improve organizational resilience.
- Departments may identify critical operational dependencies and prepare contingency measures accordingly.

9. Periodic Review and Monitoring

Risks and mitigation measures may be reviewed periodically by the Risk Management Committee and senior management. The review process may include operational, strategic, financial, compliance, cyber security, and business continuity risks. Appropriate reporting mechanisms may be established for monitoring the effectiveness of mitigation measures and implementation status.

RISK MANAGEMENT STEPS

Risk Management Step	Procedure	Expected Output
Risk Identification	• Identify potential internal and external risks that may impact the Company's objectives, operations, financial position, reputation, or compliance obligations. • Consider inputs from operational processes, finance, HR, legal, regulatory, technological, and market-related factors. • Evaluate possible scenarios, emerging risks, and business environment changes through appropriate assessment methods and expert inputs, wherever necessary.	• Risk Register • List of identified risks and scenarios • Preliminary risk assessment / SWOT analysis
Risk Analysis and Assessment	• Assess the likelihood and impact of identified risks based on qualitative and/or quantitative parameters. • Evaluate the potential effect of risks on cost, quality, timelines, operations, financial performance, compliance, and business continuity. • Classify and prioritize risks based on severity, probability, and business impact.	• Risk classification matrix • Risk impact assessment • Prioritized risk list
Risk Mitigation and Response Planning	• Develop appropriate mitigation strategies and action plans for identified risks. • Assign responsibilities to the concerned departments or officials for implementation and	• Risk mitigation plan • Responsibility matrix • Risk response and monitoring framework

Risk Management Step	Procedure	Expected Output
	monitoring of mitigation measures. • Establish timelines, review mechanisms, and escalation procedures for effective risk management. • Communicate significant risks and mitigation measures to the appropriate management levels and committees, wherever necessary.	
Risk Monitoring and Control	• Periodically review the status of identified risks and effectiveness of mitigation measures. • Monitor changes in risk exposure, control effectiveness, and implementation progress. • Review incidents, corrective actions, lessons learned, and emerging risks for continuous improvement. • Maintain appropriate documentation, reporting systems, and review mechanisms for ongoing risk monitoring.	• Risk monitoring reports • Updated risk register • Corrective action status reports • Lessons learned and improvement measures

RISK HANDLING DECISION FLOW

Stage / Decision Point	Risk Handling Action	Illustrative Measures / Outcomes
Assessment of Risk	Evaluate whether the identified risk can be avoided, transferred, mitigated, or escalated for further review.	• Risk assessment and evaluation • Identification of feasible response strategy
Risk Avoidance	Where feasible, the Company may avoid the risk by modifying business processes, operational approaches, or project requirements.	• Adopt alternate approach or process • Remove or revise specific requirements • Reduce exposure to identified risks
Risk Transfer / Deferral	Risks may be transferred, shared, outsourced, insured, or deferred to a future phase,	• Transfer risk through contractual arrangements

Stage / Decision Point	Risk Handling Action	Illustrative Measures / Outcomes
	where appropriate and commercially feasible.	• Shift implementation timelines • Outsource or subcontract activities • Defer non-critical requirements to subsequent phases
Risk Mitigation	Appropriate mitigation actions may be implemented to reduce the likelihood or impact of identified risks.	• Implement control measures • Communicate identified risks to relevant stakeholders • Periodically review mitigation actions and effectiveness • Monitor residual risk exposure
Fallback / Contingency Planning	For critical or residual risks, fallback or contingency plans may be developed to ensure business continuity and minimize disruption.	• Modify operational requirements • Develop contingency procedures • Identify alternative resources or processes • Eliminate or reduce dependency on high-risk activities
Escalation and Higher-Level Review	Risks requiring additional management attention or strategic decisions may be escalated to higher authorities or committees for review.	• Management review and intervention • Strategic decision-making • Additional monitoring and supervision
Documentation and Recording	All identified risks, mitigation measures, review status, and contingency actions may be appropriately documented and maintained.	• Update risk register/database • Maintain audit trail and records • Track mitigation and review status

FORMAT OF RISK IDENTIFICATION AND ASSESSMENT

Risk Description	Likelihood	Likely Impact Statement	Quantified Time / Cost / Other Impact	Risk Impact Level: High / Medium / low

LIKELIHOOD VS CONSEQUENCE RATING CHART
(Table for classification of Risk Occurrence and Risk Impact)

Classification of Consequences – Both Threats and Opportunities	
Rating	**Financial Impact**
High	**Financial impact on the organization is likely to exceed 25% on the value of the proposals under consideration.**
Medium	**Financial impact on the organization likely to be between 10 and 25%.**
Low	**Financial impact on the organization likely to be less than 10**