RISK MANAGEMENT POLICY

Introduction

Monarch Surveyors and Engineering Consultants Limited ("Monarch" or "the Company") operates in an environment of strategic, operational, financial, legal, reputational and technological uncertainties. Disciplined risk management is integral to achieving business objectives, safeguarding stakeholder interests and complying with Section 134(3)(n) of the Companies Act 2013, Regulation 17 **and, where applicable, Regulation 21 (Risk Management Committee)** of the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, as well as ISO 31000. This Policy sets out the Company's framework for systematically identifying, assessing, monitoring and mitigating risk.

Purpose

The Policy articulates Monarch's commitment to a structured, consistent and enterprise-wide approach to risk management. The objective is to embrace risk-informed decision-making that balances value creation with prudent risk-taking, embedding a culture in which risk considerations **including their linkage to performance evaluation and incentive structures** inform every significant decision while ensuring entrepreneurial initiatives remain within Board-approved limits.

Scope

The Policy applies to all departments, projects, subsidiaries, joint ventures and associate entities, regardless of geography or function. Every director, officer, employee, contractor, consultant, supplier and other third-party service provider acting on the Company's behalf must comply. The framework encompasses strategic, financial, operational, compliance, cybersecurity and data-privacy, environmental and reputational risks arising from internal activities and extended supply chains.

Definitions

"Risk" is the effect of uncertainty on objectives, expressed as a combination of impact and likelihood. "Risk appetite" denotes the quantum and type of risk the Board is willing to accept, articulated through qualitative statements and quantitative limits. "Risk tolerance" represents permissible variation around appetite before corrective action is required. Monarch employs a **five-point rating scale**
1 Low (Green), 2 Moderate (Yellow), 3 High (Orange), 4 Very High (Red), 5 Extreme (Crimson) applied to **individual risks and aggregated portfolio profiles**. An **emerging risk** is a newly developing or evolving threat whose full impact is not yet certain.

Policy Statement

Monarch maintains an enterprise-wide risk management framework proportionate to its size, complexity and risk profile. The framework is forward-looking, integrated into strategic planning, resource allocation and performance management, and is designed to anticipate potential events rather than merely react. All risks that could materially affect corporate objectives are escalated to the Board, which retains ultimate accountability.

Governance

The Board approves this Policy, the risk-appetite statement and any modifications, and **undertakes an annual deep-dive review of the consolidated risk register**. If a Risk Management Committee (RMC) is constituted per Regulation 21 it shares oversight with the Audit Committee; **where no RMC exists, the Audit Committee discharges its responsibilities in full**. Detailed role allocations are documented in committee charters. The Audit Committee/RMC approves the annual risk-assessment timetable and reviews quarterly updates. Executive responsibility rests with the Chief Executive Officer, while the Head of Internal Audit & Risk maintains the enterprise risk register. Functional heads own specific risks and mitigation plans aligned with appetite.

Risk Management Process

Risk identification uses horizon scanning, scenario planning, external intelligence sources, internal workshops, project-level assessments and incident trending. Risks are categorised as Strategic, Financial, Operational, Compliance, Cybersecurity & Data-privacy, Environmental and Reputational. Each risk is scored for impact and likelihood; inter-dependencies where one risk amplifies another are captured using digital risk-dashboard tools. Mitigation strategies include avoidance, reduction, transfer (insurance, hedging, outsourcing) or acceptance, with accountable owners, timelines and KPIs. Controls are tested periodically, and residual risk is re-evaluated against tolerance.

Reporting and Monitoring

The Head of Internal Audit & Risk submits a consolidated risk register **each quarter** to the Audit Committee, flagging movements, emerging threats, **overdue actions with escalation protocols**, appetite breaches and inter-dependencies. Material items are escalated to the Board immediately or at the next meeting; periodic Board-level deep dives into top risks are scheduled at least once a year. A summary of key risks forms part of the Board's Report under Section 134 (3) (n).

Continuous Improvement

Framework effectiveness is evaluated through self-assessments, internal-audit reviews, independent external evaluations and **feedback from stakeholders such as suppliers, customers, lenders and regulators**. Lessons from incidents and industry events are incorporated into revised controls, training and policy updates. Employees undergo periodic risk-awareness training.

Review of the Policy

The Policy shall be reviewed **annually** by the Audit Committee (and RMC, if in place) or immediately following any major regulatory change; amendments take effect upon Board approval.

Effective Date

This Policy is effective from **April 1, 2025** and supersedes all previous risk-management statements or procedures.