Risk Management Policy for Relim Consulting Services Limited
Effective Date: 1st January 2025

1. Purpose
Relim Services is committed to proactively identifying, assessing, and managing risks that may affect its operations, financial stability, compliance, and reputation. This policy provides a structured approach to risk management, ensuring business continuity and sustainability.

2. Scope
This policy applies to:
All employees, management, and board members.
Business partners, suppliers, and contractors.
All business operations, transactions, and projects.

3. Risk Management Objectives
Minimize potential risks that may disrupt operations or financial performance.
Ensure compliance with Kenyan laws, including the Companies Act 2015, Data Protection Act 2019, and industry regulations.
Promote a risk-aware culture among employees and stakeholders.
Strengthen business resilience and adaptability to changes in the business environment.

4. Key Risk Categories
A. Strategic Risks
Market competition and changing consumer trends.
Business model viability and scalability.
Government policies and regulatory changes.

B. Operational Risks

Supply chain disruptions.
IT system failures and cybersecurity threats.
Workplace health and safety risks.

C. Financial Risks

Cash flow shortages and liquidity issues.
Credit risks from customers and suppliers.
Fraud, theft, or financial mismanagement.

D. Compliance & Legal Risks

Non-compliance with tax, labour, and licensing regulations.
Data protection and privacy breaches.
Intellectual property infringement.

E. Reputational Risks

Negative publicity or customer complaints.
Unethical business practices.
Employee misconduct or corruption.

5. Risk Management Framework

A. Risk Identification

All employees and management must identify potential risks in their work areas.
Risks will be documented in a Risk Register.

B. Risk Assessment & Analysis

Risks will be analysed based on:
Likelihood: (Low, Medium, High)
Impact: (Minor, Moderate, Severe)
Risk Level: (Acceptable, Needs Monitoring, Requires Immediate Action)

C. Risk Mitigation & Control Measures

Develop preventive measures (e.g., cybersecurity protocols, supplier diversification).
Implement corrective actions for identified risks.
Assign responsibility for risk monitoring and response.

D. Risk Monitoring & Reporting

Employees must report emerging risks to the Managing Director.
Updates will be presented to management and stakeholders quarterly.

6. Roles & Responsibilities

A. Management

Ensure implementation of this policy.
Provide resources and training for risk management.
Make strategic decisions to mitigate high-risk areas.

B. Employees

Identify and report risks.
Follow risk mitigation procedures.
Maintain compliance with company policies.

C. Board Audit & Risk Committee

Oversee the risk management process.
Evaluate risk control strategies.
Provide recommendations to senior management.

7. Business Continuity & Crisis Management

A Business Continuity Plan (BCP) will be developed for major disruptions.
An Emergency Response Team will be established.
Regular crisis response drills will be conducted.

8. Compliance & Review

This policy will be reviewed every 3 years or when significant risks arise.
Non-compliance may result in disciplinary action or contract termination.

Approved by:
Bernard Omondi
Managing Director
1st January 2025