SATHOSA MOTORS PLC

Policy on Risk Management and Internal Controls

Sathosa Motors PLC
25, Vauxhall Street, Colombo 02

30TH SEPTEMBER 2024

1. Preamble

This policy establishes a structured and comprehensive framework for managing risks and ensuring effective internal controls within the Company, ensuring resilience in a dynamic business environment.

2. Purpose

The purpose of this policy is to safeguard the Company's assets, ensure accurate financial reporting and compliance with regulatory requirements, and support the achievement of strategic objectivesof the Company**.**

3. Scope

This policy applies to all employees, management, and the Board of Directors of Sathosa Motors PLC.

4. Definitions

4.1 Risk: The potential for events or circumstances from internal or external environment, that can adversely affect its ability to achieve its objectives, operate efficiently, and maintain financial stability.

4.2 Risk Management: The process of identifying, assessing, and managing risks to minimize their impact on the Company's objectives.

4.3 Internal Controls: Policies, procedures, and practices designed to safeguard assets, ensure the accuracy of financial reporting, and promote operational efficiency and compliance.

5. Risk Management Process

5.1 The risk management process of Sathosa Motors PLC ensures that goals are achieved through identification, assessment, and treatment and monitoring of risks. This risk management process is depicted in below diagram.

5.2 Communication and Consultation

5.2.1 The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Sathosa Motors PLC and its Subsidiaries shouldmaintain effective communication on risk management within the Group, with external parties such as suppliers, customers, and other type of clients and all the stakeholders.

5.3 Establishing Risk Context

Sathosa Motors PLC will consider following context, when managing risks:

5.3.1 External Risks - External risks are exposures that result from environmental conditions that the Company is unable to influence, such as the regulatory environment and economic conditions. Consideration should be given to the following inputs as they relate to the organization: social, regulatory, legislative, cultural, competitive, financial,technological, and the political environment.

5.3.2 Internal Risks - Internal risks are exposures that arise from the decision-making processes and the use of internal and external resources. The internal context is the internal environment in which the Company functions and seeks to achieve its objectives. Consideration should be given to factors such as:

- Strategies and plans in place and monitored to achieve objectives
- Governance, organizational structure, roles, and accountabilities
- Resourcing and capability of employees, systems, and processes
- Changes to processes or compliance obligations
- The risk tolerance and appetite of the Board

5.4 Risk Identification

5.4.1 The potential risks that could impact the Company's operations, financial performance,or reputation are identified and communicated by the process owners and the Heads ofall Departments. This includes strategic, operational, financial, and compliance levels.

5.4.2 Risk identification will be managed according to the process.

5.4.3 The Company uses following methods to identify risk at all levels.

- Periodic review on operations and processes
- Quarterly meetings with staff and teams
- Market analysis
- Financial analysis
- Regular audits
- Surveys and evaluation

5.5 Risk Assessment

5.5.1 All identified risks are analyzed at four (04) levels (extreme/high/medium/low). The Risk Registers are used to assess and evaluate the potential impact and likelihood of each identified risk and prioritize risks based on their significance and potential impact on the Company.

5.5.2 Likelihood Criteria

5.5.2.1 Likelihood of potential adverse risk events will be assessed against five criteria, ranging from Unlikely to Definite and are then rated on a scale of 1-5 as to the extentto which they impact negatively on the business.

Likelihood		**Impact**	
1	Rare	1	Insignificant
2	Unlikely	2	Minor
3	Possible	3	Moderate
4	Likely	4	Major
5	Almost Certain	5	Extraordinary

Impact	**Extraordinary**	**H**	**E**	**E**	**E**	**E**
	Major	**H**	**H**	**E**	**E**	**E**
	Moderate	**L**	**M**	**H**	**H**	**E**
	Minor	**L**	**L**	**M**	**H**	**H**
	Insignificant	**L**	**L**	**M**	**M**	**H**
		Rare	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
		Likelihood				

L- Low **M**- Medium **H**- High **E**- Extreme

5.5.3 Risk response ratings are defined as:

Extreme	• Immediate action is required to mitigate the event. Action at Senior Management and Board level is required.
High	• A priority action plan needs to be formulated and additional controls are needed to minimize the event. Action at Senior Management level is required.
Medium	• Additional actions need to be assessed, approved, and action should be taken in a routine manner to minimize the risk event. Action at operational level is required.
Low	• No specific further actions are required, hence should be managed by routine procedures.

5.6 Risk Evaluation

The Company should compare the risk found during the analysis process with risk criteria to determine whether the risk and its magnitude are acceptable or tolerable. Based on this comparison, the need for treatment will be considered.

Risk Treatment	Description
Avoid the risk	Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk.
Take the risk	Take or increase the risk in order to pursue an opportunity.
Remove the risk	Remove the risk source.
Change the risk	Modify the risk by altering its likelihood or impact through specific actions or controls.
Share the risk	Transfer some or all of the risk to a third party.
Retain the risk	Accept the risk and implementing measures to manage its potential consequences.

5.7 Risk Monitoring and Review

The Company and the Internal Audit Department should continually monitor and review the risk management procedures and compliance with the support of risk owners and the Management of Subsidiaries.

The Company should conduct the following methods for risk monitoring and review.

- Audit Committee meetings
- Monthly management meetings
- Annual key staff forum
- Regular audits

5.8 Risk Reporting and Record-keeping

The Company should record and report on risk management. Accordingly, all risk owners should document the identified risks and report to relevantauthority based on priority, including the effectiveness of management of these risks.

5.9 Risk Register

The Risk Register should detail major risks, their rating, controls, and treatments, as well as responsibilities and timeframes. Company should maintain anup-to-date Risk Register for the review of the Audit Committee.

6 Internal Controls

6.1 Control Environment

6.1.1 A comprehensive internal control framework is implemented, encompassing control activities, risk assessment, information and communication, and monitoring.

6.1.2 The Company promotes an ethical culture and strong governance practices to support the effectiveness of internal controls**.**

6.2 Control Activities

6.2.1. Segregation of Duties: Ensure proper segregation of duties to prevent conflicts of interest and reduce the risk of fraud.

6.2.2. Reconciliations: Conduct regular reconciliation for all significant financial activities and ensure the accuracy of records

6.2.3. Authorization and Approval: Establish authorization and approval processes for financial transactions, expenditures, and other significant activities**.**

6.2.4. Physical Control: Protect assets and sensitive information through physical safeguards

6.2.5. Documentation: Maintain accurate and complete documentation of transactions, processes, and controls.

6.3 Information and Communication

6.3.1. Implement and maintain information systems that support accurate financial reporting and compliance with relevant laws and regulations.

6.3.2. Ensure effective communication of internal control policies, procedures, and expectations to all employees.

6.4 Monitoring and Review

6.4.1. Routine audits are carried out by the Internal Audit Department assessing the efficiency of internal controls and identify areas for improvement.

6.4.2. Monitor compliance with internal control policies and procedures, and address any deficiencies or issues identified**.**

7 Roles and Responsibilities

7.1 Board of Directors shall have the overall responsibility for overseeing the company's risk management and internal control systems. They must conduct a review of internal controls to obtain reasonable assurance of their effectiveness and adherence. The Board is also responsible for providing oversight and guidance on risk management and internal control processes, policies and practices and as well as ensuring adequate resources are allocated.

7.2 Senior Management must be actively involved in the implementation of risk management and internal control strategies. They are responsible for ensuring that policies and procedures are followed and for reporting on risk management activities and effectiveness of internal controlto the Board of Directors.

7.3 The Audit Committee is responsible for reviewing the effectiveness of internal controls and risk management processes, ensuring that the Company's risk management and internal processesare adequate and compliant with Sri Lanka Auditing Standards. The Audit Committee shall obtain and review statements from the Heads of Business Units, who will identify theirrespective major risks and the mitigation actions taken or planned. The Committee will then recommend appropriate remedial actions to the Board.

7.4 Our risk management approach strengthens the Company's overall responsibility for managing risks, aligns with industry best practices, and enhances our internal controls. Responsibilities for effectively controlling risks are assigned across three (03) levels:

7.4.1 Risk Ownership (1st Line of defence)

Operational managers are responsible for owning and managing risks, as well as implementing corrective actions to address process and control deficiencies.

7.4.2 Risk infrastructure (2nd line of defence)

This consists of functions that monitor the implementation of effective risk management practices by operational managers. They assist risk owners in defining target risk exposure and provide adequate risk-related information throughout the Company.

7.4.3 Risk Governance and oversight (3rd line of defense)

This provides the governing body and Corporate Management with comprehensive assurance,based on the highest level of independence and objectivity, through the internal audit function.

7.5 All employees must adhere to internal control policies and procedures and report any identified risks, control deficiencies, or non-compliance issues to management. Employees are encouraged to participate in awareness programs to enhance their understanding of risk culture and internal controls. Employees who engage in training, skill development, capacity building, and adherence to the code of conduct and our attractive remuneration and compensation framework reinforce and support the Company's risk culture.

8 Training and Awareness

Employees will receive training on the Risk Management and Internal Control Policy as part of the Company's ongoing process. Ongoing training will be provided to endure understanding and compliance with updates to the policy.

9 Policy Review and Updates

9.1. Annual Review

Review and update this policy annually to ensure its continued relevance and effectiveness in managing risks and maintaining internal controls.

9.2. Continuous Improvement

Seek feedback from employees and other stakeholders to identify opportunities for improving risk management and internal control practices.

PASSED BY THE BOARD OF DIRECTORS THROUGH A CIRCULATED RESOLUTION ON 30TH SEPTEMBER 2024