SINGER FINANCE

# POLICY ON RISK MANAGEMENT AND INTERNAL CONTROL

**In Compliance with CSE Listing Rule 9.2.1 (f)**

## VERSION 2.0

## DOCUMENT AND VERSION CONTROL

| **Document Type** | **Document Name** |
|---|---|
| Policy document | Policy on Risk Management and Internal Control |

| **Document No** | **Version/Revision** |
|---|---|
| CSE Policies - 7 | 1.0 |

| **Written by** | **Contents examined by** | **Released by** |
|---|---|---|
| Arunda Silva -Senior Manager Risk and Eranda Mahagamage – Manager Internal Audit | Thushan Amarasuriya -CEO | Lasitha Dias<br>Company Secretary |

| **Approved by the Board on** |
|---|
| 24/09/2024 |

# Table of Contents

## 1. Scope and Objective

## 2. Requirement for the policy

The Risk Management and Internal Control Policy of Singer Finance (Lanka) PLC hereinafter referred as "SFL" or the "company" has been created to address and minimize the risks associated with conducting financial services business. This document will discuss and identify the risks encountered in the Company's operations and the regulatory requirements for overseeing and monitoring financial services business.

This policy encompasses both risk and internal controls. As SFL is a regulated finance company, the Risk function will fall under the purview of the Integrated Risk Management Committee (IRMC), while the internal controls will be overseen by the Board Audit Committee. The Regulatory requirements mandate the company to have comprehensive policies in both of these areas. This policy does not replicate the entirety of those policies due to their extensive nature, which encompasses the broader requirements of the Central Bank of Sri Lanka (CBSL). Instead, this policy offers an overview of the risk and internal control functions, encompassing the essential holistic aspects.

In carrying out the functions, the main type of Risks that would be faced by the company are as follows:

- Credit Risk
- Market Risk
- Liquidity and funding Risk
- Operational risk
- Strategic
- HR
- Crime and corruption/fraud risk
- IT risk (including Cyber Security & Data privacy Risk)
- Reputational risk
- Legal Risk
- Compliance Risk
- Business Risk (Macro-economic and Geopolitical risks)
- Environmental, Social and Governance Risk (ESG risk)

This document will discuss in brief how the controls are imposed to mitigate same and duties and responsibilities of each unit with monitoring authority of same. This policy is in compliance with the requirement set in Section 9 of the CSE listing rules on Corporate Governance.

## 3. Objectives of the Risk Management Policy

The primary goal is to establish guidelines for controlling, monitoring, and reporting risks that could impact the operations of SFL. Management considers risk management crucial and aims to take appropriate action to prevent any negative impact on the company's financial position.

The objectives of the policy will be achieved by

- Inculcating a risk management culture within SFL with the initiative from the framework of integrated risk management guidelines.
- To introduce best practices in the industry and benchmark the Companies risk policies.
- To record and monitor threats faced by the Company and to evaluate opportunities available in a methodical manner.
- To define the risk exposure and identify the same at required levels.
- To assist calculated risk taking and ensure conscious decisions are taken with proper evaluation.

## 4. Role of the Board of directors

The planning responsibility of risk identification and understanding made by the Board of directors will be the framework for management of risks in the Company. The required activities and the techniques will be broadly done by way of following which will address all dimensions which impact the risks.

- Management and monitoring of activities through Board Sub Committee; Integrated Risk Management committee.
- Adopting of written systems, policies and procedures which relate to management of Risks.
- Ascertaining and identifying tolerance levels/Limits of risks.
- Defining quantitative and qualitative risk goals.
- The relative behavior of risk exposures and connected outstanding in relation to capital of the Company
- Ensure compliance with the policies incorporated and the regulator requirement through a sound mechanism to monitor risk exposure.
- Introducing and directing robust systems for internal controls from time to time

## 5. Responsibilities and Users

The requirement of this policy should be applied primarily by the Board Integrated Risk Management Committee and all staff of the Company including those employed on a contract basis. Any deviations by staff will be subject to disciplinary action. Therefore, submission of accurate information on a timely basis as required by members of the Committee is considered imperative for effective implementation of this policy.

## 6. Board Integrated Risk Management Committee (BIRMC)

### 6.1 The composition and responsibilities

The primary responsibility of the BIRMC is to identify, monitor, measure, and make recommendations on the overall risk profile of the Company. The committee will operate based on the terms of reference of the BIRMC and will review the company's risk management policy and guiding principles across all risk aspects. It will also assess the company's compliance with regulatory requirements and propose systems and procedures for future risk monitoring and development to enhance risk mitigation efforts.

The committee will review the ALCO minutes, stress testing scenarios, and risk-goal monitoring. The main topics of discussion will include the identified volatility in portfolio values, and any necessary actions required will be discussed.

### 6.2 The Structure of the Committee

BIRMC shall consist of a minimum of three (03) Non-Executive Directors out of which a minimum of two (02) or the majority of the members shall be Independent Directors.

Director / Chief Executive Officer, Head of Risk, and other Key Resource Persons (KRPs) supervising broad risk categories namely Credit, Market, Operational, Information security risks and Compliance shall be invitees. The Head of Risk will serve as the secretary to the Committee.

The Head of Risk will act independently of the business units and monitoring of Credit, Market, Operational and Information security related risks will be under his purview. The Company has appointed Senior Manager Compliance (SMC), who will be the in charge for the compliance function of the Company, the SMC directly reports to BIRMC. The Committee may invite any key management personnel for participation at the meetings depending on the subject matters under discussion in the agenda.

## 7. Operational Procedures, Guidelines and Risk Goal Monitoring

The operational procedures and guidelines are established under the directive of the Board. These guidelines will in turn have to be followed at operational levels where risks are actually created by the staff who take risks on behalf of the Company in the process of providing financial services to customers or providing support services to the business units, viz front office, credit relationship, dealers, support services staff etc. The principles to follow in adopting such guidelines, policies and procedures are broadly set out below.

## 8. Credit Risk

Credit Risk is identified as the possibility of losses or impact arising due to diminution in the credit quality of borrowers or counter parties in relation to lending, settlement, and any other financial transactions. These losses could arise from default by individual, corporate, other counter parties due to their inability or unwillingness to meet the commitment. Credit Risk will arise from the Interest earning receivables of the Company.

### 8.1 Components of Good Credit Risk Management systems

- Credit policies, strategy, and process.

  Company is required to adopt policies and procedures in monitoring credit in the organization. Policies are the foundation on which Credit Risk Management of both portfolio and processes are built. The main policies/tools, which are currently used for credit management are;

- Credit Policy Manual
- Product Related Policies – (Leasing , Gold Loas, Consumer Group Loans)
- Policy on Loan Review Mechanism (LRM)
- Stress Testing Policy/Framework
- Impairment Policy
- Impairment Procedure Manual
- Delegated authority limits

New policies adopted will be vetted by the Board Credit Committee and submitted to the Board for approval. Credit strategy will be adopted according to the established objectives and goals of the Company's credit granting activities and will be according to the organization's credit appetite and the acceptable level of risk-reward tradeoff for its activities and will be initiated by Head of Risk.

### 8.2 Credit Process

Credit process is laid down in the Manual on Credit Policy and Procedure. Same is also in accordance with the internal control system of the Company. Other the delegated credit authority and their limits all other disbursements of facilities are done through an independent central credit function headed by the Senior Manager Credit. Board Credit Committee besides its functions in an advisory capacity is the approving authority for large credit facilities.

### 8.3 Credit Culture

Selection of staff and their development of expertise is especially required to establish and sustain a good credit culture. The Company will adopt best practices in the industry to ensure a good credit culture.

## 9. Market Risk, Liquidity Risk, and Interest Rate Risks

### 9.1 Market Risk Monitoring Policies

The potential impact on movements of the market prices adversely in relation to the value of a secured collateral is broadly identified as Market Risk. Since Company deals mostly in price sensitive assets and liabilities the evaluation of potential impact of the market activities will assist to identify risks that will impact on the financial activities. Any impact due to illiquidity of the instruments and the interest rate volatility which may incur due to such positions should be evaluated and prudent steps should be taken to minimize losses. Relevant tests should be done to incorporate extreme events and shocks should be captured on portfolio vulnerabilities based on market developments.

### 9.2 Market Risk Goals

Considering the level of importance of Market Risk Management, the following goals are determined currently for monitoring at the BIRMC.

i) Statutory liquid asset ratio should be maintained within the limit prescribed by the Regulatory body.
ii) Interest Rate Risk should be within the Company's internal limit
iii) Loan-to-value ratios of Gold Articles should be within the Company's internal limit
iv) Results of stress testing in relation to Liquidity and Core Capital should be within the company's appetite

## 10. Operational Risks

### 10.1 Operational Risk Management Framework

Operational Risk is intrinsic to every financial institution, and it should be an important content of our Company wide risk management framework. The framework outlines the internal operating policies of SFL Operational Risk Management Framework and sets out a context that complies with regulatory requirements as well as internal requirements towards managing Operational Risks.

Operational risk is relevant to every aspect of the Companies business and covers a wide spectrum of issues. Losses arising through fraud, unauthorized activities, errors, omission, inefficiency, system failure or from external events all fall within the operational risk definition.

Operational Risk is defined as: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

The management of Operational Risk comprises:

- Identification
- Assessment
- Monitoring & Control of Operational Risks
- Reporting

Given below are the relevant policies and procedures relevant to Operational Risk Management of the Company.

- Integrated Risk Management Policy
- Operational Risk Management Policy

### 10.2 Operational Risk Goals

Arising out of the risk indicators and guidelines, the following goals are identified under operational risks to be achieved by the Company s.

i. Operational losses not covered by Insurance over net income for the reporting period
ii. Results of Branch/Departments/IS audits carried out
iii. Report on detection of internal frauds/attempts
iv. Report on detection of external frauds/attempts
v. To maintain staff turnover ratio on acceptable level
vi. No of unplanned core Company system down times
vii Unreconciled / unidentified outstanding in suspense accounts if any

viii Availability of succession plan at strategically important/ specialized departments

ix. Total number of complaints received during the period

## 11. Information Security

"Security" in relation to information shall mean the maintaining of Confidentiality, Integrity and Availability, properties of the information, as per the following definitions:

- **Confidentiality -** Information should not be made available or be disclosed to unauthorized entities (i.e. persons, organizations, and systems)
- **Integrity** - Reliability of information will be maintained through protection from unauthorized, unintended modifications during transmission, storage, and retrieval; and
- **Availability** - Authorized users are granted timely and uninterrupted access to information. Availability will be based on the business requirement of the user.

**Company shall strive to secure information, safeguard information/ IT assets and develop efficient information systems by:**

i) Being committed to protecting Company's critical information from intentional or unintentional unauthorized disclosure, modification, or destruction throughout its lifecycle. This protection includes an appropriate level of security over the assets used to process, store, and transmit that information while aligning with the Company's strategic goals.

ii) Following information security objectives are expected to be achieved:

- Implement, enforce, and conduct periodic review of information security policies, procedures, guidelines, and checklists.
- Establish safeguards to protect the company's information/information systems from theft, abuse, Leakages, misuse, and any form of damage(s) / Potential damage(s);

- Understand the specific challenges associated with system access, and designing, deploying, and maintaining successful access controls.
- Conducted privilege / user access reviews for all critical systems annually to ensure the access controls and information security of the Company.
- Encourage management and staff to maintain an appropriate level of awareness, knowledge, and skill to allow them to minimize the occurrence and severity of information security incidents and breaches.
- Information security weaknesses and incidents are identified, recorded, and responded to in a timely manner.
- Ensure physical & logical access controls in place to enhance information security.

  i) Ensure the Company's technology infrastructure "Change Management Process" - When Company begins to use a change information resource (software, hardware, networks, system documentation, and environment) for any reason including but not limited due to system or infrastructure enhancement, it should be managed according to a specific process called a "change management processes", fixed in advance so that the transition is accomplished in an organized way in all its steps from the review to the authorization, test, implementation, and release of the changed resource;

  ii) Ensure the proper preventive and detective measures are taken against potential threats through "Patch Management". - Patches apply to many different parts of the Company information system which include operating systems, servers, routers, desktops, email clients, mobile devices, firewalls, and many other components that exist within the network infrastructure;

- Ensure availability of information systems by providing recommendations for minimum downtime.
- Ensure the utilization of storage capacity and adequate level of monitoring is being carried out to avoid unnecessary interruption.
- Ensure appropriate application, operating system, database, and network security controls are implemented and weaknesses are identified.
- Ensure all critical information for the Company is backed up and restoration testing has been conducted.
- Working with third-party cyber security specialists to enhance cyber security
- Ensure all data are classified based on information security sensitivity level and labeled with assigned classification by enforcing required policies

- Implement Mobile Devices Management requirements for Company provided Mobile phones
- Privilege Access Management system (PAM) is available to maintain administrative access management.
- Software Licensing to be purchased, and update appropriately.
- System patching, Vulnerability Assessment and Penetrating Testing (VAPT), and remediation to be attended to appropriately.

iii. Evaluate the appropriateness of technology infrastructure in order to address business requirements effectively and enhance the efficiency of business operations.

iv Proactively assess risks that may harm the Companies information systems.

v. Maintaining the compliance with any applicable legal, regulatory, contractual obligations and based on the latest industry security standards (for example: Payment Card Industry Data Security Standards and Central Company guidelines, etc.) while preserving the Company's reputation and image.

vi. Identify and report any violations of the information security policies.

Risks arising from compliance, reputational management, legal, stability and IT etc. are also considered important to be controlled for functions of financial service sector. The risks which affect the reputation should be identified and prioritized for establishing strategies to protect the reputation of the organization if we are to avoid a crisis of confidence among the stakeholders, especially the wider public, i.e. customers/depositors.

## 12. Strategic, Compliance, Legal and Information Security

### 12.1 Risk Goals to be monitored.

The following risk indicators and goals are to be monitored for the protection of relationships under the said contingencies.

**<u>On Strategic</u>**

i. Net Interest Margin should be maintained at or above the budgeted levels
ii. Annualized ROA (before Tax) should be maintained at or above the budgeted levels
iii. Annualized ROE should be maintained above the budget.
iv. Capital adequacy ratio – TIER I should be maintained above the CBSL requirement.
v. Capital adequacy ratio – TIER II should be maintained above the CBSL requirement.

vi. Cost/Income Ratio should be maintained below the budget.
vii. The YTD Deposit growth rate should be maintained above the budget.
viii. YTD lending growth rate should be maintained above the budget.
ix. Work towards improving Credit Rating.

**On Compliance**

i No of breaches reported under Submission of Regulatory / statutory returns.

ii No of reported regulatory breaches (KYC/AML ect)

iii Number of Suspicious Transactions Reported (STR) submitted to FIU.

iv Maintaining of CRIB reporting data acceptance ratio

**On Legal**

i) Legal cases against the Company which have a material impact on values.

**Information Security**

i) All baseline security standards should be achieved more than the target given by BIRMC.

**Strategic Risk Management**

The BIRMC pursues the risk indicators / goals and will make recommendation for Strategic Risk Management.

The key areas for such recommendation would be;

- Improvements to the segmentation of business mix.
- Threats identified in industries.
- Liquidity management arising out of ALCO.
- Monitoring of compliance breaches and controls to be imposed.
- Changes due to direction of the regulator.
- Recommendation from the Internal Audit based on the lapses identified in the Business Units.

## 13. Reporting Procedure

The respective Business and supporting units are required to report to the risk department on the positions of risk goals on a monthly basis. The Risk Department will compile the reports and submit them to the BIRMC with the necessary review and recommendation for detailed deliberation.

Based on the said observations and recommendations, a report will be submitted to the Board on risks goals monitored by the Company highlighting the areas of concern. If any further recommendations are made by the Board such will be notified to the relevant units for adherence. Progress of which will be reported to the next board meeting or the next BIRMC. Continuous improvement and more prudent methods of monitoring will be one of the main objectives of the Company wide risk management procedure for mitigating new threats faced by the Company. Risk Goals and the tolerance limits are reviewed periodically by BIRMC in line with the Company's overall strategic objectives and risk appetite.

## 14. Prevention and Remedies available

Company will be required to maintain adequate insurance coverage over all properties and other insurable risks. The Finance Department will be maintaining Insurance records (except for following) and will be responsible for coordinating with insurance companies and for annual renewal of policies.

- Human Resources will handle insurance of staff connected policies

## Internal Control Policy

### 1. Introduction

An effective system of internal control is vital for the success of an organization, especially financial institutions that are entrusted with public money. The internal controls refer to policies, plans and processes as affected by the Board of Directors and performed on continuous basis by the senior management and all levels of employees within the Company. The system of internal controls includes financial, operational and compliance controls. An internal control system includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed.

Internal control improvement is an ever-evolving process and needs to complement change in the operating environment. Therefore, each group in the Company will review its internal control system on an on-going basis to keep it current and effective.

### 2. Objectives of Internal Controls

The internal controls are designed to provide reasonable assurance regarding the achievement of Company's objectives and help the management to evaluate processes and manage risks.

### 3. Broad objectives of Internal Controls include:

a) To ensure efficiency and effectiveness of operations;

b) To ensure reliability, completeness and timeliness of financial and management information;

c) To ensure compliance with applicable laws, regulations, policies and procedures.

### 4. Scope

The internal control policy is applicable across the Company

### 5. Internal Control Framework

The Internal Control Policy is aligned with the Internal Control- Integrated Framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is most widely used internal control framework in the financial sector. The framework uses the bottom-up approach for risk assessment, in which risks are identified through process mapping and controls identification via developing process-flow charts.

## 6. Components of Internal Control

The SFL internal control structure consists of the following interrelated components.

- Control environment
- Risk assessment and management
- Control Activities
- Accounting, Information & Communication
- Self-Assessment & Monitoring

### 6.1 Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It reflects the overall attitude, awareness and actions of the board and management concerning the importance of control activities. It is the foundation of all other components of the internal control, providing discipline and structure. Control environment factors include;

- The integrity, ethics and competence of personnel,
- Organizational structure of the institution,
- Oversight by the Board and senior management,
- Management philosophy and operating style,
- The way management assigns responsibility, organizes and develops its personnel,
- Attention and direction provided by the Board and its committees.

Accordingly, in order for internal controls to be effective, an appropriate control environment shall demonstrate the following behaviors;

- Board and management promote high ethical & integrity standards and establish a culture that emphasizes and demonstrates to all levels of personnel the importance of internal controls.
- Board approves and periodically reviews overall business strategies & policies of the Company and ensures that these are implemented.
- Board monitors effectiveness of internal control system.
- An independent internal audit function that directly report to the Board Audit Committee (BAC), which periodically tests and assess compliance with internal control policies / procedures and reports the instances of non-compliance.
- External Auditors interact with the BAC and present the Management Letter to the Board directly.
- Board ensures that appropriate remedial actions have been taken when instances of non- compliance are reported and internal control system has been improved to avoid recurring errors/mistakes.
- Management information system provides adequate information to the Board and they have access to Company 's records, if need arises.

- Management ensures to set up internal control system across the Company to cover key risks areas to meet the Company 's objectives. Key Risk Areas include those core activities, the breakdown of which may render the Company unable to meet its obligations to customers, regulators and the shareholders.
- Delegation of authority should be performed whenever practical. However, delegation of powers should be in writing and based on the appropriate skills and experience of the employee.
- No single individual (regardless of rank, title, or function) will process a specific transaction from initiation to final authorization. This means that four eyes principle shall be strictly followed for all transactions prior to its completion
- All procedures in force should ensure that transactions are correctly processed, authorized, completed, and recorded to provide an acceptable audit trail. Procedures should also prevent accidental or intentional damage to processing systems and records.
- The hiring process should be strictly in compliance with the approved HR policies ensuring Know Your Employee (KYE) procedures which must include credentials verification on timely basis.
- Training needs are periodically assessed and extended to enhance the skill set of employees.
- Third party employee should not be allowed any duty in violation of regulatory guidelines on outsourcing.
- All information systems and activities should be strictly subject to Company 's approved IT Security Policy.
- Exercising internal controls is the responsibility of every individual employee of the Company and violation to set policies & procedures are subject to accountability.

## 6.2 Risk Assessment and Management

Risk assessment is the process that the Board and management use to identify and analyze risks which could keep the Company from achieving planned objectives. The assessment should help determine what the risks are, how they should be managed and what controls are needed.

- The Company shall identify risks to the achievement of its objectives across the entity and analyzes them as a basis for determining how these risks should be managed.
- The Company shall consider the potential for fraud in assessing risks to the achievement of objectives.
- The Company shall identify and assesses changes that could significantly impact the system of internal controls.
- The Company shall specify objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

The Company faces variety of risks that must be recognized and continually assessed. From an internal control perspective, a risk assessment should identify and evaluate the internal and

external factors that could adversely affect achievement of its performance, information and compliance objectives.

Internal factors include complexity, nature and size of operations, quality of personnel, employee turnover, objectives and goals etc. External factors include fluctuating economic conditions, changes in the industry, technological advances, degree of aggressiveness of the market and competition faced by the market participants etc. The risk identification should be done across the full spectrum of the activities, addressing measurable and non-measurable aspects of risks.

The risk evaluation is done to determine which risks are controllable and which are not. For those risks that are controllable, it must be assessed whether to accept those risks or the extent to which these could be mitigated through control procedures. For those risks that cannot be controlled, the senior management may decide whether to accept these risks or to withdraw from or reduce the level of business activity concerned. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks with the changing circumstances and conditions.

The Company shall develop a strategy for identification, quantification, aggregation, mitigation, monitoring, and reporting of operational risk. The operational risk assessment, key risk indicators, operational risk tolerance limits (thresholds) and periodic monitoring would be done in line with the Risk Management Policy and Operational Risk Management Framework of the Company.

### 6.3 Control Activities

Control Activities are the policies and procedures that help to ensure that Board and management directives are carried out. These activities help to ensure that the Board and management manage and control risks that could affect Company operating performance.

The control activities are designed and implemented to address the risk identified through the 'Risk

Assessment and Management process. The control activities involve two steps;

- Establishment of control policies and procedures.
- Verification that the control policies and procedures are being complied with.

Control activities occur throughout the organization, at all levels and in every business/function. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties. Control activities are most effective when these are made an integral part of the daily activities of all relevant personnel. Further, the duties are appropriately segregated so that personnel are not assigned conflicting responsibilities. Segregation of duties shall be built into the selection and development of control activities.

The management shall establish and maintain a system of adequate internal controls and procedures which cover all their functions in general and key risk areas in particular, for implementing strategies and policies as approved by the Board designed to provide reasonable assurance as to the integrity and reliability with respect to effectiveness of those controls and reports produced there from. All employees must ensure implementation of defined controls in discharge of their respective functions.

### 6.4 Accounting, Information & Communication

Information & Communication systems ensure that risk-taking activities are within policy guidelines and that the systems are adequately tested and reviewed.

Information and communication systems capture and impart pertinent information in a form and timeframe that enables the Board, management and employees to carry out their responsibilities.

- The Company obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
- The Company internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
- The Company communicates with external parties regarding matters affecting the functioning of other components of internal control.

Accounting systems are the methods and records that identify, assemble, analyses, classify, record, and report the transactions in accordance with prescribed formats and international best practices.

Information systems are the reports on operations, finance, and compliance-related activities. The system should cover the full range of activities in such a manner that information remains understandable and useful for audit trail. The access to information systems is to be allowed or restricted as appropriate.

Communication systems impart significant information throughout the Company so that all personnel understand their own role, correlation of their activities with others and their responsibility in the control system. Significant information is also imparted to external parties such as regulators, shareholders, and customers as per statutory and regulatory requirements.

**Effective information and communication system**

For Effective information and communication system, management will ensure following:

- On a periodic basis (at least yearly) a communication to all employees of a division shall be taken out by the respective Head advising them of the importance of internal controls in the Company and reminding them of their responsibilities in this regard.
- In addition to affecting a control assessment, business managers must foster an environment that encourages all personnel to come forward and seek help when risks and control problems are recognized. While having a risk or control problem is never a good situation, allowing it to exist and worsen before escalation to senior management and not seeking help to get issues resolved is a scenario that cannot be tolerated.
- All functions shall report issues (including control weaknesses, compliance issues and ineffectively controlled risks) in a timely manner, identified within their respective groups during the process of review of their processes/ Manuals.

## 6.5 Self-Assessment and Monitoring

Self-assessment and monitoring is an integral part of the internal control system. The process includes;

- Board and senior management oversight of the internal control, control reviews, and audit findings.
- The Company selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
- Company evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board, as appropriate.
- All departments should report issues (including control weaknesses, compliance issues and ineffectively controlled risks) in a timely manner, identified within their respective groups through any of the following sources:
  - External Auditors – Management Letter
  - Internal Audit
  - Compliance Function

- The Internal Audit Function (IAF) shall evaluate, during its periodic internal audits, the adequacy and effectiveness of self-assessment testing activities.

## 7. Internal Control Principles

Internal Control principles include following:

a) **Cover all activities:** Company shall develop internal controls which have coverage over all functions, in general, and the key risk areas (KRA) in particular. Key Risk Areas include those core activities, the breakdown of which may render the Company unable to meet its obligations to its customers, regulators, and the shareholders. Examples of key risk areas are Liquidity Risk, Interest Rate Risk, Foreign Exchange Risk, Credit Risk, Operational Risk, compliance risk, reputational risk, etc.

b) **Regular Feature:** Control activities shall be an integral part of the daily activities of Company in such a manner that it becomes ingrained in their on-going processes.

c) **Segregation of Duties:** Duties shall be divided so that no one person has complete control over a key function or activity.

d) **Authorization and Approval:** All transactions shall be authorized before recording and execution.

e) **Custodial and Security Arrangements:** Responsibility for custody of assets needs to be separated from the related record keeping.

f) **Review and Reconciliation:** Records shall be examined and reconciled regularly to determine that transactions are properly processed, approved and recorded.

g) **Physical Controls:** Equipment, inventories, cash, and other assets shall be secured physically, counted periodically, and compared with amounts shown on control records.

h) **Training and Supervision:** Qualified, well-trained and supervised employees help to ensure that control processes function properly.

i) **Documentation:** Documented policies and procedures promote employee understanding of duties and help to ensure continuity during employee absences or turnover.

j) **Communication of Internal Controls:** Approved policies and procedures shall be accessible to relevant staff for reference and implementation.

## 8. Reporting of Internal Controls

A 'Statement on Internal Controls' shall be included in the annual report of the Company. This statement should include following:

i. A statement of management's responsibilities for establishing and maintaining adequate internal controls and procedures followed by management's evaluation of the effectiveness of the Company's internal controls.

## 9. Limitations of Internal Controls

The internal control system, no matter how well designed and operated, can only provide reasonable assurance to management and the Board of Directors regarding achievement of entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that human judgment in decision-making can be faulty, and that breakdowns can occur because of such human failures as simple error or mistake. Moreover, controls can be avoided by the involvement of two or more persons, and management has the ability to override the internal control system. Another limiting factor is that even an effective internal control system can also experience a failure.

**Lasitha Dias**
**Company Secretary**

**Eraj Fernando**
**Head of Finance**

**Thushan Amarasuriya**
**CEO**