# POLICY ON

# RISK MANAGEMENT & INTERNAL CONTROLS

SARVODAYA DEVELOPMENT FINANCE PLC

**Version 1.0**

## Document Information

| | |
|---|---|
| **Document** | Policy on Risk Management & Internal Controls |
| **Author** | Head of Risk Management and OIC-IAD |
| **Department** | Risk Management & Internal Audit Departments |
| **Version** | Version 1.0 |
| **Review frequency** | Annually |
| **Document ID** | RMIC/2024/1.0 |

## Amendments & Changes

| Version | Date | Reasons for Amendments | Author |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## Authorization

| Version | Date | Reviewed by | Date | Approved by |
|---|---|---|---|---|
| 1.0 | 20.09.2024 | BIRMC | 25.09.2024 | Board of Directors |
| | | | | |
| | | | | |
| | | | | |

# Contents

1. Introduction ..... 5
**1.1 Objective** ..... 5
**1.2 Intention and Use** ..... 6
**1.3 Basis of Design** ..... 7
**1.3.1 Principles for Managing Risks** ..... 7
**1.4 Promoting Risk Integration and Developing a 'Risk Culture'** ..... 8
2. Ownership, Review and Update ..... 9
3. Overview of SDF's ERM Framework ..... 9
**3.1 Enterprise Risk Management Framework of SDF** ..... 11
4. Definitions ..... 12
5. Risk Governance Framework ..... 13
6. Risk Governance Structure ..... 14
**7.1 Management Level Committees (Executive Committees)** ..... 15
**7.2 Board Sub Committees** ..... 17
**7.3 Risk Management Department (RMD)** ..... 17
7. Risk Categorization ..... 19
8. Risk Appetite Statement (RAS) ..... 23
9. Process for Managing Risk ..... 23
A. **Risk Identification** ..... 24
B. **Risk Analysis and Measurement** ..... 24
C. **Risk Monitoring and Reporting** ..... 25
10. Risk Management & Reporting Procedure ..... 25
11. Internal Controls ..... 26
**11.1 Key Components of Internal Control** ..... 27
**a) Control Environment** ..... 27
**b) Risk Assessment** ..... 27
**c) Control Activities** ..... 27
**d) Information and Communication** ..... 28
**e) Monitoring** ..... 28
**11.2 Roles and Responsibilities** ..... 28
**11.3 Compliance** ..... 29

12. Review and Revision of Policy ..... 29

# 1. Introduction

As a financial institution engaged in offering wide range of financial products and services, the assumption and active management of financial risks are integral parts of SDF's business strategy. This implies that the core mission for risk management is adequate risk steering, as opposed to mere risk avoidance or minimization. Risk management and internal controls therefore is an integral part of the management and control system, ensuring the timely identification, analysis, measurement, management and reporting of risks. This system provides the basis for successful value-based management, including the efficient allocation of capital and the optimization of key performance measures through consistent consideration of risk-return implications.

Sarvodaya Development Finance PLC's (SDF's) risk management process is mandated by the Board of Directors and steered by the Board Integrated Risk Management Committee (BIRMC). The Board of Directors defines what levels of risk-taking are deemed adequate for SDF, taking into account all relevant limitations as well as SDF's business strategy.

On this background, the establishment of a formal governance framework for risk management at the SDF's strategic level is of central and vital importance to meet

- Internal requirements for risk information on behalf of the Board of Directors,
- Risk Based Capital and other requirements as required by the local regulator CBSL (Central Bank of Sri Lanka)

## 1.1 Objective

The objective of this Policy on Risk Management & Internal Controls of Sarvodaya Development Finance Plc (SDF) is to ensure all business risks are prudently identified, analyzed and managed in accordance with the Principles for Managing Risks (Section 1.3.1) set out in this Risk Management Policy & Procedure.

An appropriate and effective risk management system ensures that the different types of Risks and their impacts are identified and evaluated at an early stage and that mitigation plans and measures are in place where necessary to handle the identified risks and to prevent the accumulation of such risks including the ensuing negative impact / consequences of such risks.

Through proper implementation of an **Enterprise Risk Management System**, SDF works towards the following goals:

- Development of a risk culture that fosters awareness of risks and a common understanding of risks across functions and departments.
- Capital protection, both for internal as well as regulatory purposes.
- Limitation of earnings volatility.
- Risk-based performance measurement and decision-making.
- Ability to act proactively or to respond quickly and effectively to adverse events.
- Better understanding of risks for competitive advantage.
- Increase transparency and optimize information flows between business functions, control functions, the Management Committee and the Board of Directors.

### 1.2 Intention and Use

This Risk Management Policy & Procedure is supplemental to detailed provisions that are in place in SDF's Policies and should be reviewed annually in response to an event or change in circumstances.

It is the intention of this Risk Management Policy & Procedure to assist in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of SDF and will help to:

- ensure that information about risks derived from the risk management process is adequately and consistently reported and used as a basis for objective-setting, decision-making and accountability at all relevant organizational / business unit levels;
- designate and monitor accountabilities and responsibilities for the managing of risks;
- ensure necessary resources are available to assist those accountable and responsible for managing risks;
- facilitate the measurement and reporting of organizational / business unit risk management performances.

The Risk Management Policy & Procedure of SDF is aligned to its policies in that it:

- sets baseline expectations in relation to critical areas;

- provides guidance to business units of the desired policies of the company.

Each business unit in the company should interpret the Risk Management Policy & Procedure in the context of its own business environment and identify and implement, integrate and continuously improve processes for managing /mitigating these identified risks.

## 1.3 Basis of Design

This Risk Management Policy & Procedure should be applied:

- throughout the life of an organization;
- to a wide range of activities, including strategies and decisions, operations, business processes, its functions, projects, products, services and assets;
- to any type of risk, whatever its nature, whether having positive or negative consequences.

### *1.3.1 Principles for Managing Risks*

In implementing this ERM Framework, the following Principles for Managing Risks should be applied:

| | Principle | Application |
|---|---|---|
| 1. | RM is an integral part of all organizational activities | Risk management is not a stand-alone activity that is separate from SDF's main activities and processes. Risk management is part of the responsibilities of management and an integral part of all organizational processes, including strategic planning and all project and change management processes. |
| 2. | RM is structured and comprehensive | A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results. |
| 3. | RM is based on best available information | The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgment. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modeling used or the possibility of divergence among experts. |
| 4. | RM is customized | Risk Management is aligned with the SDF's external and internal context and risk profile. |

| | | |
|---|---|---|
| 5. | RM takes human and cultural factors into account | Risk Management recognizes the capabilities, perceptions and intensions of external and internal people that can facilitate or hinder achievement of SDF's objectives. |
| 6. | RM is transparent and inclusive | Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels in SDF, ensures that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria. |
| 7. | RM is dynamic and responsive to change | Risk Management continually senses and responds to change to external and internal factors based on social / political / environmental and economic events which occur including context and knowledge change, the monitoring and review of risks would be constant, including monitoring of the emergence of new risks, including changes to existing risk parameters. |
| 8. | RM facilitates continual improvement of the Organization | SDF is committed to developing and implementing strategies to improve the risk management maturity alongside all other aspects of the company. |

### 1.4 Promoting Risk Integration and Developing a 'Risk Culture'

SDF's Risk Management Policy & Procedure will act as the platform for the integration of risk management processes within SDF's business objectives. Risk integration means risk identification, its analysis, evaluation of mitigants and its application as practiced in all businesses and decision-making processes.

When risk management is integrated with business processes, it will help to develop a robust 'risk culture' that will be characterized by the following key attributes:

- risk and risk management are proactively involved in daily corporate judgment;
- the risk management process is transparent, known and understood by all internal and external stakeholders;
- the value of consistent understanding of risk tolerances levels and how risk management affects daily decisions, is constantly endorsed by the board of directors down to line-level managers.

Following on, a risk management culture will support SDF to embrace the full potential of adopting robust risk management policies and to be proactive about understanding and managing risks, leading to benefits in the following areas:

- ability to respond proactively to business crises;
- organizational survival/longevity;
- reputation/brand protection;
- improved financial performances.
- conform to CBSL Directive / Regulations

Ongoing awareness programs and communication, training and education is an on-going necessity / action activity which shall be conducted regularly / consistently to ensure continuous commitment and support by all staff for its risk management. **Managing risk is a shared responsibility**. It is inevitable that SDF will face risks, but these risks should be effectively managed to increase risk-adjusted returns, improve strategic judgement and avoid extraordinary losses.

## 2. Ownership, Review and Update

The Board of Directors holds the ownership for the risk policy and defines the risk strategy for the Company. The risk strategy reflects the risk appetite and tolerance and, thereby, the desired level of confidence in achieving business targets.

The SDF's risk management function and the Board sub-committee on integrated risk management are responsible for the proposed revisions to this Risk Policy document.

The Board of Directors reviews and approves the policy statement on an annual basis.

## 3. Overview of SDF's ERM Framework

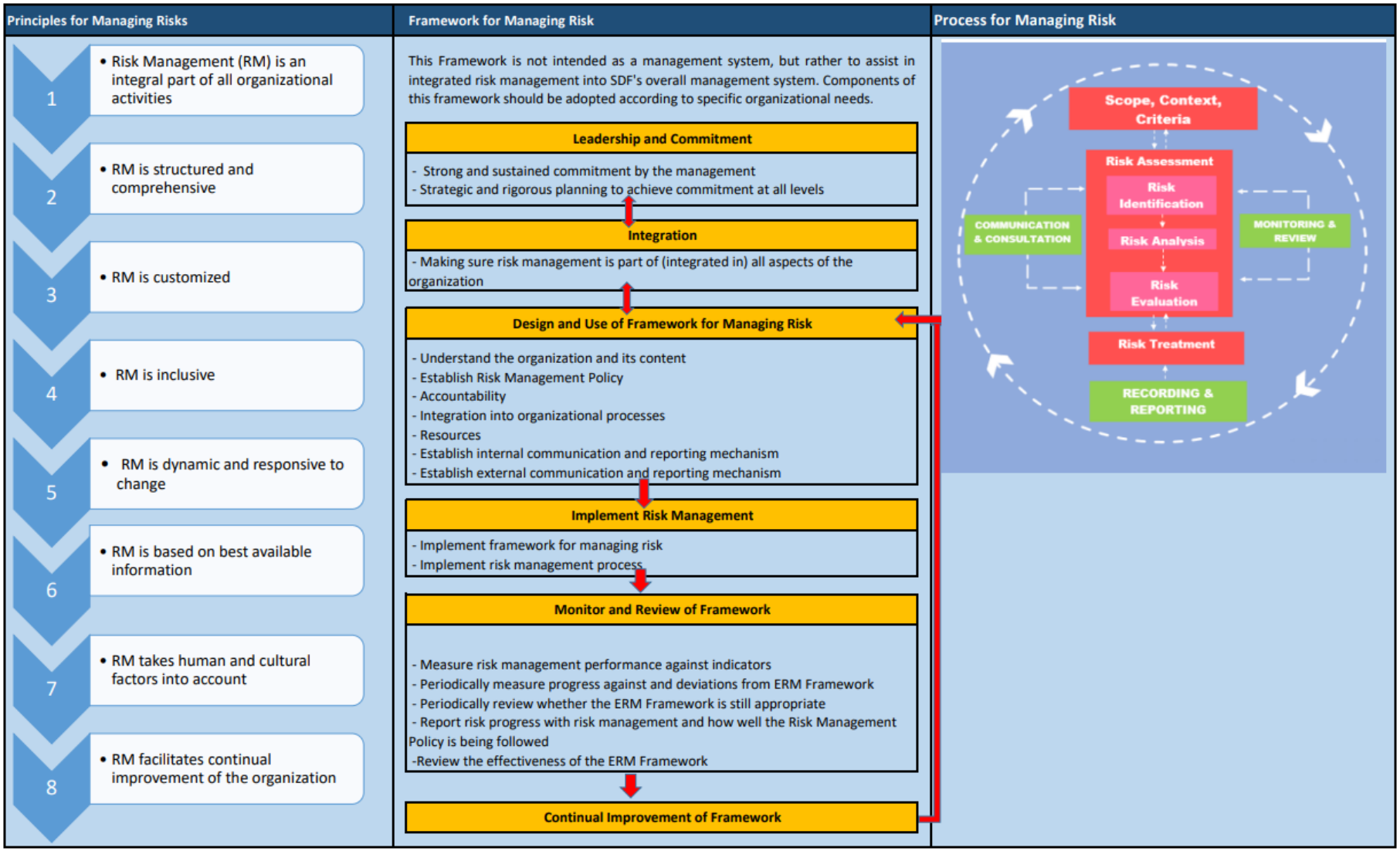
The success of risk management will depend on the effectiveness of the management framework providing the culture, foundations and the process arrangements that will embed it throughout SDF at all levels.

SDF's ERM Framework assists in managing risks effectively through the application of the risk management process at varying levels and within SDF's specific business context.

The ERM Framework ensures that information about risk derived [identified] from the risk management process is adequately reported and used as a backdrop for decision-making and accountability at all relevant organizational levels.

An overview of the components of the ERM Framework for managing risk and the way in which they interrelate is shown below (next page).

### 3.1 Enterprise Risk Management Framework of SDF



## 4. Definitions

### 4.1 Risk

Risk is any event, situation, or circumstance, which, if it occurred, would adversely impact the achievement of objective of the SDF including the failure to capitalize on opportunities and possibly resulting in financial losses.

### 4.2 Risk Management

Risk Management is the process of systematically identifying, quantifying, and managing all risks and opportunities that can affect achievement of a corporation's strategic and financial goals.

### 4.3 Risk Strategy of SDF

The Risk Strategy of the SDF defines the Company's standpoint towards dealing with various risks associated with the business. It includes the Company's decision on the risk tolerance levels, and acceptance, avoidance or transfer of risks faced by the SDF.

### 4.4 Risk Assessment

Risk Assessment is defined as the overall process of risk analysis and evaluation based on impact & likelihood.

### 4.5 Risk Estimation

Risk Estimation is the process of quantification of risks and qualitative factors also taken in to consideration.

### 4.6 Risk Tolerance/Risk Appetite

Risk tolerance or Risk appetite indicates the maximum quantum of risk which the SDF is willing to take as determined from time to time in accordance with the Risk Strategy of the SDF.

### 4.7 Risk Description

A Risk Description is a comprehensive collection of information about a particular risk recorded in a structured manner.

### 4.8 Risk Database

The 'Risk Database' is a database for recording the risks encountered at various locations and levels in a standardized format of Risk Description

## 5. Risk Governance Framework

The Company has adopted a "**three lines of defence**" governance framework**.** The three lines of defence framework operate as follows;

| 1st Line of Defence | 2nd Line of Defence | 3rd Line of Defence |
|---|---|---|
| **Business lines/ Corporate Functions** | **Risk Management & Control Functions** | **Assurance Function** |
| Ownership for the day-to-day management of risks | Direction for Risk Management and Compliance, facilitating high level of risk awareness throughout the organisation | Independent and objective assurance on the Risk Management processes and practices in place |
| - CEO<br>- Senior Management<br>- Management Committees<br>- Business Units | - BIRMC<br>- Board Credit Committee (BCC)<br>- RMD<br>- Compliance Department | - BAC<br>- External Auditor<br>- Internal Audit Department |

I. **First line of defence** represents the Risk Owners [Business Owners]. They have the first and direct responsibility for the assessment and control of the Company's risks (management committees, management and staff attached to different business units);

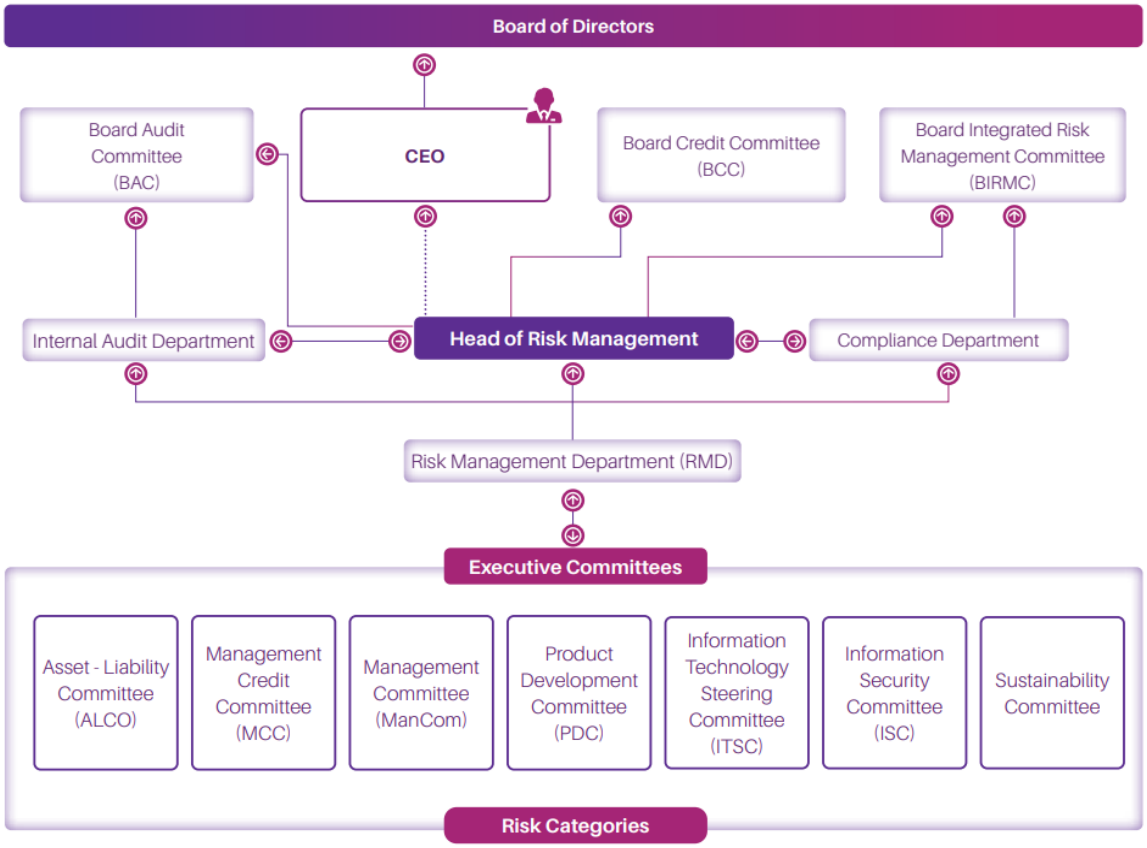
II. **Second line of defence** comprises of units providing the independent risk oversight. They co-ordinate, facilitate and oversee the effectiveness and integrity of the Company's Risk Management Framework (BIRMC, Board Credit Committee, Risk Management Department and Compliance Department);

III. **Third line of defence** provides independent review of effectiveness of risk management practices and internal control framework and recommend for improvements where necessary (Internal and External Audit, and Board Audit Committee).

## 6. Risk Governance Structure

The Company's Board of Directors is responsible for developing the overall risk strategy, including; supervision of the Risk Management Framework, approval of the overall Risk Management Policy and overseeing and challenging the risk levels to which the Company is exposed, while ensuring compliance with laws and regulations. The Board has delegated its authorities to the Board Sub-Committees and hence the overall adequacy and effectiveness of the Risk Management Framework is managed by the Board Integrated Risk Management Committee (BIRMC) while the Board Audit Committee (BAC) is providing an assurance to the Board. These sub-committees comprise of Non-Executive, Independent Directors and Non-Executive, Non-Independent Directors. In order to increase the soundness and effectiveness of the supervision, SDF has formed Management Level Committees such as Asset- Liability Committee (ALCO), Management Credit Committee (MCC), Management Committee (ManCom), Product Development Committee (PDC) and Information Technology Steering Committee (ITSC), Information security Committee (ISC) and Sustainability Committee. These Committees comprise of senior level staff members who are in charge of key business functions.

Acting within the authority delegated by the Board, these committees review specific risk areas and receive regular reports on risk management, internal controls, portfolio trends, policies, limits and standards.



## 7.1 Management Level Committees (Executive Committees)

### a. Assets and Liabilities Management Committee (ALCO)

Assets and Liabilities Management Committee (ALCO) is chaired by the Chief Executive Officer (CEO) and comprises of senior management personnel who are in charge of Finance, Risk Management, Credit, Fund Mobilisation, Operations and Compliance. The Committee meets regularly to monitor and manage the assets and liabilities of the Company and also to monitor the overall liquidity position to keep the Company's liquidity at healthy levels, review the SDF's cost of funds as well as will approve the rates of lending and deposit products whilst satisfying regulatory requirements. ALCO is responsible for identifying, managing and controlling risks in executing the business strategy of the Company and mainly focuses on Interest Rate Risk and Liquidity Risk while maintaining profitability.

### b. Management Credit Committee (MCC)

Credit Committee is chaired by the **CEO** and comprises of **Head of Credit, Head of Finance** or higher designated in charge of Finance & Planning, **Head of Recoveries** and **Head of Risk Management**. The Committee meets regularly to monitor and manage the Company's lending portfolio, asset quality and recovery actions. The Committee also periodically reviews Company's Credit Policy and lending rates to different business segments, in line with prevailing market conditions and industry dynamics and the new rates will be forwarded for the approval of the ALCO. MCC approves credit facilities within its delegated authority and reviews the methodologies for assessing credit risk and monitors concentration risk.

### c. Management Committee (MANCOM)

ManCom oversees the overall strategy and the new developments in the risk environments to take timely precautions and corrective measures. The Committee is headed by the **CEO and comprises of the Senior Management.**

### d. Product Development Committee (PDC)

The Company has formed a Product Development Committee for new products including Senior Management positions, internal stakeholders from business units and other `ad hoc' members with expertise in applicable functions such as credit, operations, legal, information technology, information security, audit, risk management, and compliance. PDC is chaired by the Chief Operating Officer (COO). The Committee shall be responsible for the design, implementation, and ongoing monitoring

of the new activities.

**e. Information Technology Steering Committee (ITSC)**

The primary role of the ITSC is to exercise oversight and governance over SDF's IT function. The Committee is authorized to take decisions to improve or secure Information Resources, within the context of the Delegation of Authority assigned by the Board of Directors to the Chair. The committee is chaired by the Chief Executive Officer and will be facilitated by the Head of IT ("HOIT") and / or Senior Manager IT ("SMIT") who will serve as the Committee Secretary. Permanent Invitees to the Committee will be the Chief Operating Officer (COO), the Head of Risk Management, the Compliance Officer and the Head of Operations & Administration.

**f. Information Security Committee (ISC)**

The prime objective of the ISC is to oversee the information security and technology resilience of the Company and would be responsible for both the strategic and operational aspects of information security and technology risk management. The ISC is chaired by the CEO. The Chief Operating Officer (COO), Head of Operations and Head of IT shall be the other ex-officio members of ISC. Head of Risk Management and Compliance Officer will be permanent invitees to ISC. Head of Legal and Head of Human Resource Management shall be required to attend as co-opted members whenever a matter relating to their arears is to be discussed. Head of Internal Audit is invited to present internal audit findings on information security at least on a quarterly basis. The Committee reports to the Board of Directors through BIRMC.

**g. Sustainability Committee**

The Committee would be responsible for overseeing sustainable strategy and environmental practice of the Company and ESG risk Management while adhering to the SDF's Sustainable Development policy safeguarding the Company's sustainable success and long term viability. The Committee comprises of COO, Head of Credit, Head of Strategic Planning, Head of Operations and Administration, Head of Risk Management and Compliance Officer where the Committee would be headed by the COO. Upon the requirement, the Committee can invite any other member from the Senior Management, Product Heads and etc.

## 7.2 Board Sub Committees

### a. Board Audit Committee [BAC]

Audit committee is a formally constituted sub-committee of the main Board, and consists of minimum 3 Board members who are Non-Executive Directors and majority shall be independent directors with necessary qualifications and experience relevant to the scope of the BAC. The chairperson of BAC shall be an independent director who possesses qualifications and experience in accountancy and/or audit. The primary function of the committee is to assist the Board to fulfill its stewardship responsibilities with regard to financial reporting requirements and information requirements of the Companies Act and other relevant financial reporting regulations and requirements. It also has oversight responsibility for reviewing the effectiveness of internal control and risk management systems. The Committee assesses the independence and performance of the Company's auditors, both internal and external auditors.

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

The Board has delegated its authority to Integrated Risk Management Committee, which is responsible for developing and monitoring the Company's risk management policies. The Committee is headed by an Independent Non-Executive Director and comprises of two more Non-Executive Directors. The Board members appointed to BIRMC shall be non-executive directors with knowledge and experience in banking, finance, risk management issues and practices. The Chief Executive Officer, Head of Risk Management and key management personnel supervising broad risk categories i.e. credit, market, liquidity, operational and strategic risks may attend the meetings upon invitation. Meetings of BIRMC are held regularly, and the Board of Directors are duly updated of its activities.

### c. Board Credit Committee (BCC)

BCC oversees the management of credit quality of the lending portfolio and recoveries actions. The Committee is chaired by a Non-Executive Independent Director and comprises of another two Non-Executive Directors and the CEO, Head of Credit, Head of Finance or higher designated in charge of Finance & Planning, Head of Recoveries and Head of Risk Management, Compliance Officer and Head of Legal or higher designated in charge of Legal are invitees to the BCC.

## 7.3 Risk Management Department (RMD)

The Risk Management Department provides an independent oversight function, acting as a 2nd line of defence

within the Company. RMD is tasked with the responsibility of assisting the business units and functional departments in identifying and managing the risks related to their respective operations and processes and independently monitoring the status and effectiveness of the mitigation action plans. RMD is headed by Head of Risk Management who directly reports to the Chairman of the BIRMC and also has an administrative reporting to the CEO.

**Main duties and responsibilities of the RMD**

a) Develop and update the Company's risk management policy and other risk management-related policies.

b) Coordinate and facilitate the training of the Company's staff to recognize risks in their work so as to foster a strong risk culture.

c) Provide and enhance tools and methods for quantitative and qualitative risk measurement.

d) Propose the Company's risk management development plan and ensure that developments are at the minimum in line with local regulatory requirements.

e) Support regulatory issues that affect risk management (capital adequacy rules, minimum requirements for risk management).

f) Evaluate and / or recommend risk mitigation strategies, track and follow-up all risk mitigation actions taken.

g) Provide an independent view on the risk-return impacts of plans and decisions and provide comments and recommendations for planning and decision processes.

h) Consolidate risk related reports and prepare regular and ad-hoc reports for the BIRMC and Board of Directors.

i) Collaborate with the Company's other control functions to achieve efficient, timely and consistent communication to the Company's management, reducing potential overlap.

j) Review of ALL approved Product Papers and its implementation of terms and conditions including the periodic (annually or once in two years) review of the different products and services, which are being offered by SDF for potential risks [current & future] and risk mitigants.

**The Risk Management Department has the following rights in order to carry out its duties:**

a) Right of access to all premises of the Company and the right to inspect all correspondences, files, records, accounts and all other documents held by the Company as necessary to perform its duties.

b) Right to interview and / or require staff of the Company to supply information and explanations as is necessary for the performance of its duties.

## 7. Risk Categorization

The most appropriate and significant risks to SDF can be broadly classified in to the following categories.

### 7.1 CREDIT RISK

Credit risk is the risk of financial loss to the Company if a borrower or counterparty to a financial instrument, fails to meet its contractual obligations, and arises principally from the Company's loans and advances to customers/other Companies and investments in debt securities.

Credit Risk constitutes the Company's largest risk exposure category. This can be broadly categorized into two types: Default and Concentration risk.

**7.1.1** **Default risk** as the risk of the potential financial loss resulting from the failure of customer or counterparty to meet its debt or contractual obligations and arises principally from the Company's loans and advances to customers.

**7.1.2** **Concentration risk** is the credit exposure being concentrated as a result of excessive build-up of exposure to a single counterparty, industry, product, geographical location or insufficient diversification.

**7.1.3** **Settlement risk** is the risk of loss arising from trading/investment activities when there is a mutual undertaking to deliver on a progressive basis,

*For example when the Company enters in to a reverse-repo transaction with a primary dealer, counterparty could fail to fulfill its contractual obligations by delivering the assigned security to the Company's custodian account after Company had advanced money.*

The management of credit risks are included in the Credit Risk Management Policy**.**

### 7.2 LIQUIDITY RISK

The risk of loss resulting from the danger that short-term current or future payment obligations cannot be met or can only be met on the basis of altered conditions, along with the risk that in the case of a liquidity crisis of the Company, refinancing is only possible at higher interest rates or that assets may have to be liquidated at a discount. Liquidity risk for a financial institution can take two forms as follows.

**7.2.1** **Transaction liquidity risk** is the risk of fluctuating price of an asset adversely in the act of buying or selling it. Company's transaction liquidity risk is low if assets can be liquidated without volatility of price.

**7.2.2** **Funding liquidity risk** means the Company's inability to finance assets continuously at an acceptable borrowing rate. Funding liquidity risk generally arises when creditors (including depositors) either withdraw credit balances or change the terms on which it is granted in such a way that the credit balances are no longer profitable for SDF to retain. Funding liquidity risk would increase if the Company's credit quality is, or at least perceived to be, deteriorating, but also due to financial conditions as a whole are deteriorating.

The management of liquidity risks is included in Company's Asset and Liability Management Policy & Liquidity Investment Policy.

### 7.3 MARKET RISK

Market risk refers to the possible losses to the Company that could arise from changes in market variables like interest rates, exchange rates, equity prices and commodity prices. Among them, interest rate risk and commodity risk which have been identified as the most critical risks given Company's business profile.

**7.3.1** **Interest rate risk** is a key constitute of the market risk exposure of the Company due to adverse and unanticipated movements in future market interest rates.

Excessive movements in market interest rate could result in severe volatility to Company's net interest income and net interest margins. Company's exposure to interest rate risk is primarily associated with factors such as;

- **Reprising risk** arising from a fixed rate-borrowing portfolio where reprising frequency is different to that of the lending portfolio.
- **Yield curve risk** arising from unanticipated shifts of the market yield curve.

**7.3.2** **Commodity price risk** refers to the uncertainties of future market values and of the size of the future income, caused by the fluctuation in the prices of commodities/gold. Commodity risk could arise from either of adverse movements in the world prices, exchange rates movements, which are basic differences between local and world prices [Arbitrage].

**7.3.3** **Equity risk** is the risk of loss based on market changes in the value of equity investments.

**7.3.4** **Exchange rate** risk is the risk of loss as a result of unhedged exposure to volatility in the local (LKR) exchange rate with other major currencies. Exchange risk could materialize as an indirect risk too, affecting local gold prices resulting in exaggerated commodity risk.

### 7.4 OPERATIONAL RISK

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events (Basel II definition). Management of operational risk is integrated across the functions since occurrence of one such risk may compound another.

Operational risk may result in a financial loss and a reputation risk to the Company. Company broadly identifies, assesses and aims to mitigate the following operational risk categories:

- Internal fraud
- External fraud
- Work place safety
- Business disruptions
- Process risk
- Damage to physical assets

The SDF's Whistle Blowing Policy and Fraud Prevention Policy will set guidelines and procedure in minimizing operational risks and the Company conducts special training programs to minimize the gaps identified in the practices.

### 7.5 REPUTATIONAL RISK

The risk of loss caused by a decline in the reputation of the Company from the point of view of its stakeholders - shareholders, customers, staff, business partners or the general public. Reputational risk can be a consequence of losses in all risk categories such as market or credit risks, as well as a cause for them.

### 7.6 HUMAN RESOURCE RISK

Human Resource risks are events that prevent employees from fulfilling their responsibilities and thus keep the business from operating at full efficiency. Human resource risks include but are not limited to;

- Employee turnover [Attrition Rate]
- poor employee management practices
- unexpected temporary leave
- management error/incompetence
- disability (temporary or permanent) death
- Succession

### 7.7 STRATEGIC RISK

The risk of an unexpected negative change in the Company value, arising from the adverse effect of top-level decisions on both business strategies and its implementation. This risk is a function of the compatibility between strategic goals, the business strategies developed to achieve those goals and the resources deployed against these goals. Strategic risk also includes the capacity / ability of the management to effectively analyze and incorporate external factors, which could impact the future direction of the Company.

### 7.8 INFORMATION TECHNOLOGY RISK

The risk associated with the ownership, use, processing, operation, involvement and adoption of information systems, information technology and technical infrastructure has been identified as IT risk by the Company. This includes but not limited to events such as fraudulent & malicious hacking of the core system / system, breakdowns, failures or interruptions which result in a system downtime, frauds through errors and system manipulations, technological obsolescence and insufficient infrastructure to support business volumes, falling behind competitors in terms of information technology.

Company has identified information as a vital business resource and a key asset to the organization. Hence, the potential of a threat exploiting the vulnerabilities of this valuable and important asset can cause adverse impact to the business operation ranging from simple inconvenience to catastrophic in scale.

### 7.9 CAPITAL ADEQUACY RISK

For a financial Institution, capital is a buffer against insolvency. It is available to absorb unforeseen losses so that the Company can remain in business as a `going-concern'. The more capital the Company has relative to the risks it takes, the more confident the stakeholders are that it will meet its obligations to them. Capital adequacy risk arises from Company's inability to maintain the required amount of capital, which is perceived to be adequate to absorb any unexpected losses. The Company's capital management objectives can be summarized as follows:

- Maintain sufficient capital to meet minimum regulatory capital requirements.
- Hold sufficient capital to support the Company's risk appetite.
- Allocate capital to businesses to support the Company's strategic objectives.
- Ensure that the Company maintains capital in order to achieve debt rating objectives and to withstand the impact of potential stress events.

### 7.10 ENVIRONMENTAL, SOCIAL AND GOVERNANCE (ESG) RISK

ESG Risks include a company's environmental, social, and governance factors that could cause a reputation or financial harm to the Company. With the ESG Risk Management, SDF targets to safeguard its sustainable

success and long term viability.

SDF has recognized the significance of alignment with the United Nations' Sustainable Development Goals and the Roadmap for Sustainable Development issued by the CBSL. Being into development financing and impact financing, SDF believes it can play a bigger role in the transition of Sri Lanka towards a green, inclusive, and balanced economy. As SDF is really passionate about the sustainability, it targets in promoting businesses that are greener, climate friendly and socially inclusive through providing financial assistance and ultimately managing environmental, social, and governance (ESG) Risks associated with these projects.

### 7.11 LEGAL / REGULATORY RISK

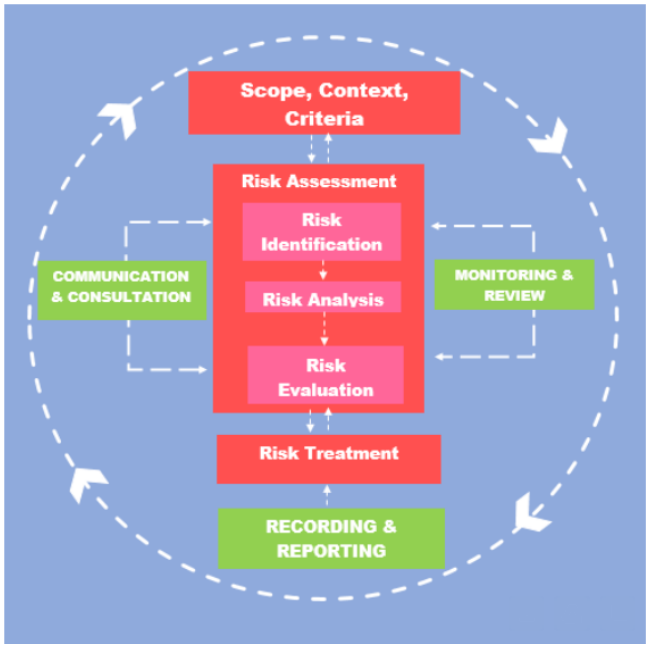
Legal/Regulatory risk is the risk of loss caused by non-compliance with existing or new legislation or supervisory regulations, disadvantageous changes to existing laws or supervisory regulations. Furthermore, legal risk includes losses due to ambiguity of laws or unfavorable contract clauses and loose contracts.

## 8. Risk Appetite Statement (RAS)

Risk appetite are types of risks and the aggregate amount of risks that the Company is prepared to be exposed to at any given point in time which is approved by the Board of Directors. After a careful consideration of the regulatory requirements, capital, funding and liquidity position, strategic objectives and the Risk Management Framework, the Company has put in place a risk appetite statement, which clearly defines the Company's risk appetite and the strategic risk objectives. SDF's Risk Appetite Statement is in line with the Company's Board approved Strategic Plan and the Annual Budget.

## 9. Process for Managing Risk

The following diagram illustrates the process for managing risk that the corporate risk management is to facilitate / coordinate with respective Heads of Business Units/ Departments. It is important to be mindful that the risk management process should be governed by the Principles for Managing Risks **(Section 1.3.1)**.




Each activity of the process will be elaborated in subsequent sections of this policy and procedure.

A. **Risk Identification**

In the context of risk identification, all existing risk categories, their sub-risks as well as their risk sources within the Company's business are determined and clearly distinguished from each other on an on-going basis. New risks can occur, given that the business environment is constantly changing and that new products are being developed and brought into the market. Early and comprehensive identification of risk is an essential element for the early warning system.

Before commencing business with new products, types of business and in new markets, the risks inherent in them and the resultant effects on risk management must be identified.

B. **Risk Analysis and Measurement**

Following on from risk identification, risks are analysed and measured using quantitative as well as qualitative risk-appropriate methods and procedures. The methods used are verified continuously using sensitivity analysis, stress tests, back testing and validation tests.

Interdependencies are to be taken into account, and risk concentrations or accumulation risks are to be continuously analyzed and evaluated.

In the qualitative risk Database, a Risk Score would be assigned for each risk event based on the Business Impact and the Likelihood (Probability) of occurring the respective threats and vulnerabilities which would

be determined as per the same methodology mentioned in the Technology Risk Management Framework of the Company.

C. **Risk Monitoring and Reporting**

The quantifiable risks are restricted by risk limits. The development of risk limits for controlling and monitoring risk positions, risk exposure in particular to avoid risk concentrations for sectors, customers and security types forms an essential part of the Company's risk approach.

All non-quantifiable risks are managed and limited via appropriate approaches or methods.

Monitoring ensures that the risk management decision is implemented appropriately and on timely manner. It includes both the monitoring of deviations from the prescribed risk limits and the monitoring of methods, procedures and processes used for quantifiable and non-quantifiable risks.

## 10. Risk Management & Reporting Procedure

Risk Management & Reporting (**RMR**) procedure allows the RMD and the Head of Risk Management to identify and assess risks affecting the entire business on an on-going basis.

a) RMR procedure starts with the initial identification of key risks concerning each business unit/function. Risk identification is a collective exercise carried out with the active participation and contribution of the respective Business Heads / HoDs (Risk Owners) at least once in two months where RMD's role primarily is to facilitate the process.

b) For quantifiable risks, Key Risk Indicators (KRIs) are defined and tolerance levels are set for monitoring purposes. KRIs should be evaluated on regular basis for appropriateness and relevance. Any new identified KRIs should be added to enhance effective risk monitoring. A comprehensive set of KRIs are prepared on a monthly basis and reviewed by Head of Risk Management. Any risk highlighted is communicated to the relevant HoDs and executive leadership of the Company to mitigate the negative consequences.

c) For qualitative non-quantifiable risks, RMD should initiate and formulate risk mitigation plans together with the respective business divisions. For agreed mitigation actions clear timelines should be set for completion and responsibilities should be assigned.

d) RMD is responsible for submitting the Key Risk Indicators to the members of IRMC on a monthly basis, which should include the status of compliance with the KRI tolerance levels.

e) Head of Risk Management is responsible for escalating any proposed mitigation strategy beyond the scope/authority of the business units/ HoD or RMD to the executive leadership and seek necessary approvals for the implementation.

f) RMD should regularly communicate with the risk owners for the purpose of monitoring KRIs and ensure the implementation of agreed mitigation strategies. Risk owners are responsible for providing all necessary information to the RMD and Head of Risk Management to facilitate independent supervision.

g) Head of Risk Management is responsible for submitting Risk Database, Top Risks and Key Risk Indicators based on the RMR procedure to the Board IRMC in once in two months.

h) Head of Risk Management is responsible for submitting summarized version of the Corporate Risk Profile (Top Risks) and KRIs Report to the Board of Directors for the subsequent Board meeting after BIRMC being held.

All employees of the Company have an obligation to report irregularities of which they become aware and to disclose any information which they believe shows serious maladministration or wrongdoing within the Company. A failure to do so shall constitute willful suppression/concealing of material facts detrimental to the Company and shall be grounds for disciplinary action.

## 11. Internal Controls

Company has formed an Internal Audit Department (IAD) which functions as an independent function and performs the 3rd line of Defense. The IAD directly reports to the Board Audit Committee (BAC).

The objectives of the IAD are:

- Safeguard the assets of the company.
- Ensure the integrity of financial information.
- Support compliance with relevant laws and regulations.
- Minimize financial and operational risks.

- Promote accountability and transparency in company operations.
- Protect shareholders' investments.
- Assess the adequacy and effectiveness of the already set internal controls and provide recommendations to enhance the adequacy and effectiveness of the internal controls.
- Audit the adherence to the Board approved policies and procedures to build uniformity and to avoid/mitigate malpractices.

### 11.1 Key Components of Internal Control

Sarvodaya Development Finance PLC shall implement and maintain the following components as part of its internal control framework:

#### *a) Control Environment*

The control environment sets the tone for the Company. It includes the ethical values, management philosophy, and corporate governance structure of Sarvodaya Development Finance PLC.

- A culture of honesty and integrity shall be promoted at all levels.
- The Board of Directors and the management team shall provide oversight and direction to ensure the establishment and maintenance of effective internal controls.

#### *b) Risk Assessment*

Internal controls shall be designed based on the identification and assessment of financial, operational, and compliance risks.

This includes:

- Continuous risk assessment at the entity, division, and activity levels.
- Regular updates on risk management to ensure controls remain relevant to emerging threats.

#### *c) Control Activities*

Control activities are policies and procedures that help ensure that management's directives are carried out. They include:

- Segregation of duties to prevent fraud and errors.
- Authorization and approval processes to ensure that only legitimate transactions are recorded.
- Regular reconciliations and reviews of financial records.
- Physical security of assets such as cash, cheques, and fixed assets.

### *d) Information and Communication*

Effective internal control relies on timely and accurate information:

- Clear communication channels shall be established to allow reporting of financial information and risks.
- Employees shall be informed of their roles and responsibilities in maintaining internal control.

### *e) Monitoring*

Continuous monitoring of the internal control system is essential to ensure its effectiveness. This will be achieved through:

- Regular internal audits conducted by the Internal Audit Department to assess the adequacy and effectiveness of internal controls.
- Management reviews and corrective action plans for identified deficiencies.

## 11.2 Roles and Responsibilities

#### a) Board of Directors

- Approve and oversee the implementation of the internal control policy.
- Monitor the overall effectiveness of the internal control system.

#### b) Board Audit Committee

- Review and evaluate the adequacy of internal controls.
- Ensure that the internal control framework aligns with the company's objectives and risk appetite.

#### c) Senior Management

- Implement and maintain effective internal controls within their areas of responsibility.
- Ensure compliance with internal control procedures.

#### d) Internal Audit Department

- Conduct independent evaluations of the effectiveness of internal controls.
- Report control weaknesses and provide recommendations for improvement.

**e) All Employees**

- Understand and comply with the internal control procedures relevant to their roles.
- Report control weaknesses or irregularities to the appropriate authority.

### 11.3 Compliance

Non-compliance with this policy will result in disciplinary action in line with company procedures.

## 12. Review and Revision of Policy

This policy shall be reviewed as required by changes in regulatory requirements or the operational environment. The Board of Directors must approve any significant changes to this policy based on the recommendation of the BIRMC.