SPANDANA SPHOORTY FINANCIAL LIMITED

RISK MANAGEMENT POLICY

Version V

Document Control

a. Document Information

File(s) Name	Risk Management Policy
Effective from	November 11, 2015

b. Document Approval / Ratification

Approving Authority	Date of Meeting	Status of Approval / Ratification
Risk Management Committee and Board of Directors	January 27, 2020 June 2, 2020 May 22, 2021 October 17, 2022	Review and approval

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Risk is an integral part of the Company's business and sound risk management is critical to the success. As a financial intermediary, the Company is exposed to risks that are particular to its lending and the environment within which it operates. The Company has identified and implemented comprehensive policies and procedures to assess, monitor and manage risk throughout the Company.

1.2. The risk management process is continuously reviewed, improved and adapted in the context of changing risk scenario and the agility of the risk management process is monitored and reviewed for its appropriateness in the changing risk landscape. The process of continuous evaluation of risks includes taking stock of the risk landscape on an event-driven basis.

2. PURPOSE AND SCOPE OF THE POLICY

2.1. Risk Management Policy Framework aims to establish basic principles and general framework for the control and management of risks which may exist or arise in the Company. The underlying premise of the risk management framework is to maximise stakeholders' value. While the Company faces uncertainties and risks, the challenge for the Company board and management is to determine, as to what extent uncertainty is acceptable in order to strive to grow stakeholder value. Risk Management is essential to this as it focuses on long-term sustainability of the Company.

3. RISK MANAGEMENT PROCESS

3.1. At the Company, risk management is a systematic process that comprises well-defined steps. When these steps are taken in sequence, they support better decision making and enable greater insights into risks. However, the risk management process does not end with monitoring and controlling risk; it is an on- going function. Further, it is not a linear process, but rather an on-going iterative process. The steps are part of an interactive and dynamic flow of information from the field to the head office (and management) and back to the field.

3.2. Identification, assessment, prioritisation and mitigation of risks

Members of the management including heads of the operations (JLG/ SP Heads), heads of back-end control functions (IT/MIS, HR, Accounts/Finance and Legal and Secretarial Department) shall bear the primary responsibility to identify risks in functional area(s) for which they are responsible (i.e. for which they are Risk Owners; Risk Owner is defined as the person responsible for managing a particular risk). The front-line business operations are responsible for assessment and control of credit risk whereas back-end control functions are responsible for identification, assessment and control of operational, liquidity and market risks. These risk owners/department heads provide the "first line of defence" in the risk governance framework. The risk owners shall inform about new risks pertaining to their work area and the consequences if not managed proactively, to the Chief Risk Officer.

In addition to the first line of defence, the Risk Management Department (second line of defence) plays a key role in identifying, assessing and managing the overall risks faced by the institution. It acts as the Risk Manager. The role of the Risk Management is to establish internal controls by scanning across all risk dimensions and to continuously identify, assess and prioritise the risk independent of the Risk Owners. Besides reporting to the Risk Management Committee (RMC) on Risk Management updates, he/she shall also apprise the Committee of the new risks identified, their severity and thus priority level. Chief Risk Officer, who shall not be a direct part of the operational command chain, shall play a critical role at taking operational exposures by evaluating policies and procedures across different functions from the perspective of risk management.

3.3. Develop strategies and tactics to manage risks

The Board determines the risk appetite as an integral part of choosing a business strategy for the Company. The business strategy needs to be developed and continuously brought in line with the risk appetite. Risk appetite statement of the Company indicates the maximum risk the institution is willing to take. The Board takes care of regulatory limits while determining the risk appetite including capital adequacy norms. The risk appetite statement of the Company shall be reassessed regularly-at least once a year-and more often if required-in view of changes in the business environment and as measures of risks.

The Board approves policies for measurement and on-going assessment of risks and monitors the Company's adherence to them. The management team identifies key indicators and ratios that need to be tracked and analysed regularly to assess company's exposure to risks.

Department heads with support from the Chief Risk Officer shall develop sound procedures and operational guidelines to mitigate each risk within their work area to the level defined by RMC. Operations and field staff may be consulted on the suggested policies and procedures to ensure their feasibility and cost-effectiveness. The Chief Risk Officer shall support the management team in development of strategies and tactics to manage risks.

3.4. Implement policies and assign responsibilities

Once suitable control measures are in place line managers shall oversee implementation of controls and monitor risks over time. Every staff is responsible for managing and monitoring the identified risk(s) that fall into his/her work area.

3.5. Test effectiveness and evaluate results

Board of the Company shall regularly review the operating results to assess whether the current policies and procedures produce the desired outcome(s) and at the same time adequately manage risks. Some indicators shall require weekly or monthly monitoring, while others shall require less frequent monitoring. Where results may suggest a need for some changes to policies and procedures and possibly identify new risk exposures, the department heads shall suggest new risk control measures.

Internal Audit's role in Risk Management is to assess the effectiveness with which the controls are addressed. Internal audit department shall serve as the control of controls

It is important to note that risk identification and assessment is both the responsibility of the 'risk owner' or the business function(s). Simultaneously, it is also a function of the Risk Management to identify the risk independent of the risk owners. Based on risk management progress reports and internal audit findings, the RMC shall review risk management policies for necessary adjustments.

3.6. Revise policies and procedures

Based on the risk reporting and internal audit findings, RMC with the assistance of Risk Management Department shall review Risk Management Policy for necessary adjustments. After the new controls are implemented, its effectiveness must be evaluated for any further improvements that can be brought about.

In a nutshell, the risk management feedback loop is an interactive and continuous process to ensure that the management is in-tune with the actual events and that the Company responds in a timely manner to any changes in its internal or external business environment.

4. RISK MANAGEMENT GOVERNANCE

4.1. Company's risk culture is based on a set of guiding principles which act as a compass to direct every employee's way of operating:

- Every employee is a risk manager
- Policy driven systems and processes where risks are openly discussed and which shape individual behaviours.

4.2. At the organisation level, the Board is responsible for overall risk management and it does so through the Risk Management Committee (RMC). The Board defines the overall risk appetite of the Company by setting limits and standards. Individual and departmental targets are in line with the risk appetite and the risk principles as established by various Board approved policies. Company has following three lines of defense for maintaining the risk culture:

4.2.1. *1st Line of Defense (Business Units):* Ultimate responsibility for day-to-day execution of controls, policies and compliance with laws, regulations. Perform in accordance with various policies and overall risk controls – Ownership of Risk. As the first line of defense, department heads (including frontline business and control functions) own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies. These department heads are responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. The first line of defense identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives. The first line of defense provides management with the assurance that robust internal controls are in place and being executed to avoid loss to the organisation.

4.2.2. *2nd Line of Defense (Risk Management & Compliance Function):* It is the owner of Risk management policies / Models. It shall ensure risks are identified, assessed, managed and reported. It sets and monitors Risk limits. It also provides the Board / management with all relevant risk related information. This line of defense provides assurance through oversight that internal controls are being properly designed and enforced for effective risk management. The oversight is guaranteed through inspection of whether the internal controls are effectively being implemented and there is compliance to risk management policies, procedures, and regulatory requirements. Risk management function facilitates and monitors the implementation of effective risk management practices by the operational management. Risk management function also defines and reviews risk policies and thresholds and provides guidance and directions for implementing the policies and for monitoring their proper execution.

4.2.3. *3rd Line of Defense (Internal Audit):* Oversees the internal control framework of the institution, including the Risk Control and Compliance functions. Provides Assurance of Effectiveness and adequacy of risk management practices to Board. This represents internal audit that offers independent challenge to organisational operations and oversight function and lends additional assurance to risk management.

4.3. In light of the three lines of defense, day-to-day management and monitoring of risks takes place by the respective department. The Chief Risk Officer who reports back on risks to RMC further supports this function. RMC, with support from the Chief Risk Officer, provides assurance to stakeholders through its oversight of risk management and by ensuring compliance to organisational risk management policies. Further, it also helps in defining and developing risk management policies and processes and defines the Company's risk appetite. Additional assurance to compliance is provided through internal and external audit of the Company.

Individual business functions of the Company are responsible for monitoring different types of risk and share the monitoring reports with the Chief Risk Officer.

5. Risk Types Managed Under the Policy

As a microfinance institution, the Company faces different types of risks. The Risk Management Policy covers broad categories of risks like Credit Risk, Operational Risk, Liquidity Risk, etc.

5.1. Credit Risk

Credit risk is the most important risk category for the Company. Credit risk for the Company refers to the possibility of its borrowers or other contractual counterparties not being able to honour their loan obligations. It includes risk arising from borrower's late repayment or non-repayment of the loan obligations. In case of the Company, apart from borrowers, contractual counterparty may also be banks where the Company subscribes to fixed deposits to access funds for on-lending purpose (especially under business correspondent model). Such defaults lead to loss of income for the microfinance institutions as they fail to collect interest and outright losses in case the principal amount given as a loan is not repaid. The Company needs to identify and manage credit risk arising out of individual transactions as well as losses of a

significant portion of the loan portfolio. Elements of credit risk are addressed in the operations manual of the Company.

Loan Portfolio
The Company has well- established risk identification and measurement systems for individual loans as outlined in the above section. However, it is equally important that overall loan portfolio of the institution is analyzed separately from the perspective of risk management and decision-making. Portfolio credit quality is measured by focusing on Portfolio-at-Risk (PAR), Vintage Analysis, etc.

Portfolio Concentration Limits
Concentration risk is the risk posed to a financial institution by any single or group of exposures that have the potential to produce losses large enough to threaten the ability of the institution to continue operating as a going concern. For example, a microfinance institution may have a concentration of loans in a certain geographic area. If that area experiences an economic downturn, an unexpected volume of defaults might occur, which could result in significant losses or failure of the institution. By the very nature of microfinance, some degree of concentration risk is inherent in the methodology; geographically, within their customer/member base, and by the products they specialise in and offer. The smaller the geographic area served, the more limited the customer base, and the fewer the number of products offered all this adds up to increased concentration risk. Concentration risk can also manifest in asset categories or within asset categories.

Mitigation framework
The Company aims to avoid concentration in both its loan portfolio and borrowings. To mitigate the concentration risk, the Company has a well-defined geographic and lender dependence norm.

5.1.1. ***Geographic Concentration Norms***

In order to mitigate the risk of external intervention, concentration in any particular state, district or branch, as well as to manage non-payment risk, the Company has following limits:

A. Portfolio Outstanding Caps:

– Cap on Loan Portfolio Outstanding for Unsecured Loans:

- Gross Loan Portfolio at State-level shall not exceed 20.0% of the Company's total portfolio. Each state shall ensure that its Gross Loan Portfolio shall not exceed 75% of the total net worth of the Company.
- Micro Credit Unsecured Loan Portfolio in the state of Andhra Pradesh shall not exceed 6% of Gross Loan Portfolio of the Company.
- Gross Loan Portfolio at the District-level shall not exceed 2.0% of the Company's total portfolio and 5.0% of the Company's net-worth respectively.
- Gross Loan Portfolio at the Branch-level shall not exceed 1% of the Company's net worth.
- Up to 5% of the operating branches may go up to 1.5% of the Company's net worth. 2 months allowed for branch to come back within limits if this is breached.

The caps are subject to tolerance limit of 10% over and above the exposure cap.

B. Disbursement Caps:

- The disbursement limits stipulate each state to entail less than 20.0% of the total disbursements of the Company.
- Each district to entail less than 3.3% of the total disbursements of the Company;
- Each branch to entail less than 1% of the total disbursements for the Company excluding non-micro finance branches.

  The caps are subject to tolerance limit of 10% over and above the exposure cap.

5.1.2. ***Political Risk***

The Company recognises political risk as one of the major risks facing the industry and believes that political risk can be mitigated through responsible lending, consistently following the fundamentals of micro finance, maintaining uncompromising discipline and client engagement.

A. Continue to remain rural focussed:

The Company intends to continue building on this competitive landscape and remain Rural. The Company shall like to maintain 85% microfinance portfolio from rural. The floor is subject to tolerance limit of 5% below this.

B. Robust Customer Grievance Redressal (CGR)

Spandana has a well-defined and fully automated Complaint Grievance Redressal Mechanism (CGRM) for ensuring timely redressal. The Company has also established a dedicated follow-up team and quality team which ensures timely closure and quality of the calls.

C. Avoidance of over-indebtedness and multiple borrowing among its borrowers:

Adherence to KYC Policy, mandatory Credit Bureau checks and automated systems ensure the seamless implementation of RBI regulation stipulated to MFIs with controls, thereby avoiding over-indebtedness and multiple borrowing among the Company's borrowers.

Instant Credit Bureau check is done and the clients are informed about the outcome and the reasons in case of rejection. The Company follows a more stringent 2 lender norms while approving a loan.

D. Establishing appropriate collection practices by employees:

Design and implement the collection practices, in alignment with the RBI and SRO guidelines and regulatory frameworks. The Company has been conducting Client Protection awareness programmes for its employees in vernacular languages with greater focus on treating client with utmost respect.

Monitoring and Control

The Company's sustainability lies in establishing adequate procedures to effectively monitor and control the credit function within established guidelines. The Company strives to develop and implement comprehensive procedures and information systems to effectively monitor and control risks inherent in its credit portfolio.

5.2. Operational Risk

Operational Risk is defined as the possibility of losses resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risks include, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Reputational risk could arise since the Company deals with vulnerable, financially inexperienced clients. When internal controls and codes of conduct fail, the damage to the reputation of a responsible microfinance provider like the Company can be substantial. Hence, for the purposes of this Policy, reputational risk has been considered as a part of operational risk.

5.2.1. Types of Operational Risk Events Relevant to the Company

There are several types of operational risk (OR) events which the Company could face. Any OR incident can be classified into one of the following top-level categories:

S. No.	Operational Risks	Examples
1.	Internal fraud	Intentional misreporting of positions, employee theft, ghost loans to non-existing clients siphoned off by business executives
2.	External fraud	Robbery, forgery, damage through computer hacking, clients misrepresenting their situation and obtaining a loan that they have no intention of paying back.
3.	Employment practices and workplace safety	Staff compensation claims, violation of employee health and safety rules, discrimination and sexual harassment claims and general liability for damages incurred by staff.
4.	Clients, products and business practices	Misuse of confidential customer information, marketing of unauthorised or inappropriate products, omission or incorrect disclosure of effective rates, abusive collection practices
5.	Damage due to Natural/man-made events	Fires, floods, vandalism, earthquakes, terrorism
6.	Business Disruption and System Failures	Hardware and software failure, utility failures, telecommunication problems, massive staff absence due to epidemic or political unrest.
7.	Execution, Delivery and Process Management	Data entry errors, collateral management failures, incomplete legal documentation, unapproved access granted to client accounts and vendor disputes.
8.	IT platform and procedure related risk	Disaster Recovery & business continuity plan failure, AMC deficiency, software upgrade, user credential reset, IS audit compliance etc.

5.2.2. Sources of Operational Risks at the Company

Operational risk events can occur when there are inadequacies or failures due to:

Internal Factors

A. People

The management of human resources and employee behaviour can become a major source of operational risk. Poorly trained or overstretched employees may expose the Company to operational risk (for example, via processing errors). Understanding of the mission and vision

of the Company, confidence in and respect for the institution as well as adherence to policies and strategies are key for effective use of human resources. In addition, the continuous availability of employees, or the Company's ability to onboard fresh skills, can influence its ability to recover from interruptions to continuity of its operations. The Company strives to develop an appropriate risk culture in which employees are aware of operational risks and are encouraged to learn from their mistakes.

B. Process and Systems
The Company's operations are supported by many different systems and processes, such as IT systems, human resource management systems, credit, market, insurance and liquidity risk management systems and even operational risk management systems.
These systems may have many different components, each of which require the operation of various processes. For example, the credit risk management system of the Company should and does include processes for the identification, measurement, monitoring and control of credit risk. Complex or poorly designed systems and processes can give rise to operational losses, either because they are unfit for the purpose, or because they malfunction. As a result, the Company may experience a wide range of problems, including settlement-processing errors, fraud and information security failures. In addition, the increasing automation of systems and the Company's reliance on IT has the potential to transform risks from minor manual processing errors to major systematic failures.

External Factors
A. Disruptive Events
Such events include fire, flooding, earthquakes, terrorist actions, vandalism, power failures, etc. The Company should assess the occurrence of such potential risks and design and put in place disaster recovery systems and procedures, with a view to ensuring business continuity. Against the monetary loss derived from such events, the Company should evaluate potential cost and acquire proper insurance.

B. Outsourcing of Services
The Company may use services of external parties for performing various tasks. Outsourcing arrangements require careful management if they are to yield benefits. If these arrangements are not managed adequately, the degree of operational risk faced by the Company may increase as is also the institution's dependency upon the use of consultants/third parties for activities that may be more effectively developed internally.

Responsibilities of the Stakeholders
Below mentioned are necessary organisational arrangements for managing operational risks in the Company in addition to those defined in Risk Management Governance section:
• The Risk Management Committee is the board level counterpart for all risk dimensions including operational risk exposures.
• The "three lines of defense" in operational risk are implemented in the Company

Mitigation and control
The core business of the Company is to provide collateral-free loans in rural areas, and consequently, requires enhanced operational risk management. To mitigate the operational risk, the Company adopts the following strategy.

A. *Product and process Design*
The Company shall ensure compliance to the client selection criteria, which shall mitigate the risk of loans disbursing to fake borrowers/ghost borrowers etc.

1. Own house is mandatory for new clients. This will ensure clients not migrating after taking multiple loans and defaulting their loans.
2. Only one member in the household is given loan: This is strictly followed as multiple loans at a household level leads to clients defaulting and running away.

B. Cap on number of loans disbursed

Maximum number of loans disbursed in a Branch is capped at 600 per month. This cap is to ensure quality appraisals, proper documentation and clear explanation of the product and policy and terms and conditions to the borrower. This restriction is built in the system and a Branch shall not be able to save loans over and above 600 in a month.

In case any Branch has sufficient manpower and demand for disbursement of loans above 600 in a month, then the Branch shall take approval in writing. Incentives pertaining to Loan Disbursement shall only be released post 100% of branch audit.

C. Avoid the risk of fake borrowers through e-KYC and borrowers taking multiple loans by submitting fake KYC documents

With the emphasis on avoiding fake KYC documents, the Company is in the process of necessary regulatory approvals and license for the Aadhaar-based biometric identification (e-KYC) of clients. Through e-KYC, fake Aadhaar shall be avoided and it shall reduce turnaround time for loan disbursements. The Company is also moving towards e-sign and instant disbursement. The Company believes e-KYC helps in mitigating the risk of fake borrowers, in addition to immediate member authentication.

D. Strict Transfer Policy

i) Credit Assistants and Branch Managers are not allowed to work in the same location for more than 18 months. Similarly, Cluster Managers are not allowed to stay in the same location for more than 24 months. Divisional Managers, Assistant Managers-Internal Audit & Managers – Internal Audit and AVP/VP are not allowed to work in the same location for more than 24 months. HR tracks employees who have completed the tenure as mentioned herein every month and they are transferred to another location during the transfer cycles in April and September every year.

ii) The minimum distance between the native place and the employees place of posting shall be 70 kms, except for Kerala and Goa where the minimum distance is 20 kms.

iii) The employee to be transferred should not have worked for more than 90 days with the employees of the branch to which he is proposed for transfer.

iv) The employee has not worked in that branch earlier during his/her employment at the Company during the last 3 years.

v) Transfer of two employees at the same time from same branch should not be done as it may affect operations at branch. Hence the gap of 30 days to be maintained between transfer of two employees from the same branch.

vi) CAs &BMs are not transferred from one branch to another branch of the same cluster.

vii) There shall be no mutual transfers of employees between branches.

viii) Two employees of same native Mandal shall not work at the same branch at the same time.

ix) Employee is not transferred within less than 10 months of his stint at current location. Exception can be given to staff who are excess as per the caseload and who are placed at a long distance.

x) Friends and relatives shall not be placed/transferred to the same branch.

xi) No two staff in a Branch can spend more than 6 months together and they are rotated in such a way that no two employees together work in the same location for more than 6 months.

New employees are not hired from restricted areas. On the basis of previous experiences, few areas are identified as restricted areas. They are hired with an exception of Cluster Manager level employee doing thorough background check.

E. Control on risk of frauds and theft while carrying cash

There is a possibility of losing cash by employees doing frauds/running away with cash and losing cash through theft/robbery. Strict cash management policy ensures minimizing this risk.

Employees carry cash 1) from Bank Branch to our Branch after withdrawing cash for loan disbursement 2) Centre Meetings to Branch as they bring collections. These risks are mitigated / minimized by strictly adhering the internal controls

Employees running away with cash from centre meetings/collection points	Per day recovery by one Credit Assistant is capped at 150 borrowers. However, there may be cases when branches may have temporary staff shortage on account of forced attrition or attrition without prior intimation. In all such cases, within relieving timelines, alternative staff is posted to the branches to contain dependence risk.
Cash transfers between Branches	This risk is mitigated as cash transfers are not allowed. All branches shall have a bank account duly operated by the authorized representatives of the Company. Exception: Branch with no active bank account. Even if the Branch does not have bank account, nearby Branch shall issue cheque;
Cash theft from branches	Branches are advised to maintain zero cash balance. Cluster Manager should stay in the branch if the cash balance exceeds Rs.50,000. Given that gradually the caseload at branches is growing and average AUM per branch has almost doubled for seasoned branches, the limit is proposed to be enhanced to Rs.2,00,000. CM/ DM shall be desired to stay at the branch if the cash balance exceeds Rs.2,00,000.
Cash theft in field	In places, where the risk of robbery is very high, opened multiple accounts in all available Bank branches and Credit Assistants are advised to deposit cash in the nearby bank Branch and not carry cash to Branch.

5.2.3. Risk Identification and Measurement

Risk & Control Self-Assessment (RCSA)

The objective of RCSA is to discover vulnerabilities and potential exposures to operational risk in a mostly qualitative, forward-looking approach. Where possible, RCSAs also attempt to estimate the frequency and loss severity of the potential exposures that have been identified.

Scope of RCSA

RCSA goes beyond the credit related processes and covers all organisational areas in the Company like, Operations, HR, IT, Finance, Compliance, etc.

Process

The Chief Risk Officer shall be responsible for initiating the RCSA process every year and documenting the results. RCSA process involves three stages, namely risk identification, risk assessment, and control evaluation.

a) Risk Identification

The Risk Management Department shall conduct structured individual discussions with all functional heads, branch managers from sample branches and area managers to identify key operational risks faced by the Company.

The following is an indicative agenda for proposed RCSA discussions:

- Presentation of previous RCSA findings and risk mitigation strategies
- Assess implementation of risk mitigation strategies (as finalised during the senior management team meetings)
- Identify operational risks and inefficiencies faced in different departments
- Understand existing risk mitigation/control strategies
- Identify gaps in the existing control strategies
- Suggest risk mitigation strategies

b) Risk Assessment

After the identification of risk, Risk Management team shall assess risks, in consultation with functional heads, of likelihood and impact; the scoring based on the following matrices shall be done after that. After scoring, the total Risk Score for each risk shall be calculated by multiplying frequency score with the score for severity. After the arrival of final scores, all operational risks faced by each functional area shall be mapped to determine the top risks faced by the Company. The outcome of this exercise is shared with all the functional heads for their feedback and comments.

Matrix for likelihood of OR events

Likelihood/Frequency	Definition	Description
1	Unlikely/Low	The risk is seen as unlikely to occur in the near future (2-3 years). The chances of occurrence of a risk event are less than 0.33 per year (i.e. less than or equal to one event every three years).
2	Likely/Medium	The risk is seen as likely to occur in the near future. The chances of occurrence of a risk event are between 0.33 to 0.66 per year (i.e. more than one event every three years)

Likelihood/Frequency	Definition	Description
3	Certain/High	The risk is expected to occur in the near future. The chances of occurrence of a risk event are greater than 0.66 per year (i.e. equal to one event every three years or more than this).

Matrix for impact or severity of OR events

Impact/Severity	Definition	Description
1	Negligible/Low	The risk shall not substantively impact the Company's operations and shall not impede the achievement of business objectives, causing minimal damage to the Company's reputation. The impact on the Company's assets or income from such risk event is less than Rs.1 lakh per year
2	Moderate/Medium	The risk shall cause some elements of the business objectives to be delayed or not achieved, causing potential damage to the Company's reputation. The impact on the Company's assets or income from such risk event is between Rs.1 lakh and Rs.5 lakh per year.
3	Critical/High	The risk shall substantively impact the Company's operations and shall cause the business objectives to not be achieved, causing damage to the Company's reputation. The impact on the Company's assets or income from such risk event is more than Rs.5 lakh per year.

c) Control Evaluation

For each operational risk identified during the RSCA workshop, the Chief Risk Officer shall identify controls that are in place and can potentially mitigate the risk. This shall be done on the basis of discussions with the concerned functional heads and details about existing control mechanisms are documented in detail.
After identification of controls, the Chief Risk Officer on the basis of discussions with the concerned functional head shall assess whether the controls are working as intended and identifies any gaps in control measures. Gaps in control measures are also documented in the RCSA tool. RCSA workshop's participants conduct qualitative assessment of control gaps and proceed to rank residual risk.

Residual Risks

The Chief Risk Officer shall reassess the identified operational risks, after applying the identified control measures, using the same impact and likelihood scales. After application of the existing control mechanism, the residual levels of risk are rated as High, Medium or Low.

Risk Owners

Each functional head is the risk owner for the identified operational risks related to his functional area or department. For all residual risks in the high or medium categories, the respective risk owners and the Chief Risk Officer discuss corrective strategies / risk mitigation strategies (along with the management team) and timelines to address the risks.

Monitoring of Control Improvements

The Chief Risk Officer shall monitor corrective actions taken by the functional heads and shall analyse if those actions provide the intended results. The Chief Risk Officer shall also monitor the implementation timeline of the corrective actions.

Report Results

RCSA results shall be incorporated into quarterly operational risk report to the Risk Management Committee (RMC).

Review and Maintenance of Key Risk Indicators

Effectiveness of key risk indicators and their threshold levels shall be done annually. If there are other indicators, which can be measured and recorded and are predictive of risk, the Chief Risk Officer may propose the inclusion of these indicators to RMC for approval. RMC shall discuss and approve threshold levels of different risk indicators on the basis of recommendations made by the management team (functional heads and the MD & CEO) and the Chief Risk Officer. Following sources of information to identify relevant KRIs for the Company is normally done:

- Historical internal loss events (Loss event database);
- Risk and Control Self - Assessment (RCSA) results;
- Internal audit findings;
- Regulatory inspection findings; and
- discussions with business functions

The Risk Management Department shall coordinate with different functional heads to capture the performance of the Company on all of these indicators.

5.2.4. ***Operational Risk Incidents Collection/Loss Event Database***

The Company shall record information pertaining to operational risk incidents in a bid to establish a well-structured database of materialized OR events that have or may eventually lead to an avoidable financial loss or expense. This database shall also help in the detection of vulnerabilities and allow the Company to better target risk management actions that shall mitigate operational risk. The Chief Risk Officer shall be the owner of this database and shall coordinate with functional heads and the internal audit head to ensure integrity and completeness of data.

Operational Risks faced by the Company

Operational Risk Category	Operational Risks
People and Business Processes	• Staff fraud • Staff turnover • Multiple lending to same client • Low capability of staff • Inadequate functionality – supporting software • High client dropout rate
IT/Systems	• Systems for data security • System breakdown

Operational Risk Category	Operational Risks
	• IT infrastructure not aligned to business needs • Inadequate systems and processes for vendor management • IT Policy not updated • Insufficient/ untested business continuity processes • Outsourcing risk • Inadequate systems for backup of data
External Events	• Third party provider failure • Natural disaster • Power outage • War and social unrest • External theft or fraud • Competition • Regulatory changes

*5.2.5.**Key Risk Indicators (KRIs)***

S. N.	Functional Area/Department		Indicators	Thresholds	Data Source	Frequency
1	Operational Risk	Human Resource	Staff turnover at the branch level Department (Confirmed operation's staffs)	<=10%	HRMS, HR Dept.	Quarterly
2			Staff turnover at the middle management level (up to VP)	<=5%	HRMS, HR Dept.	Quarterly
3			Staff turnover at the senior management level	<=5%	HRMS, HR Dept.	Quarterly
4			No. of disciplinary cases excluding frauds	0	HRMS, HR Dept.	Quarterly
5			No. of staff complaints unresolved	0	HRMS, HR Dept.	Quarterly
6			No. of incidents of staff fraud	0	HRMS, HR Dept.	Quarterly
7			No. of customers' complaints against staff	0	Operations	Quarterly
8	Credit Risk		No. of clients with multiple loans from more than two other MFIs	0	MIS	Quarterly
9			% of unsatisfactory CGTs/GRTs/LUCs following Internal Audit reviews (% within the audited sample)	<=10%	MIS	Quarterly
10			No. of incidents of staff override credit bureau reports per branch	0	IT	Quarterly
11	Operational Risk		Incidents of Cash held in excess of operational limit	<=3	Branch Accounts	Monthly
12			No. of client complaints unresolved	<=50	Complaints Dept.	Quarterly
13			No. of unresolved client complaints within 7 days of registering	<=10	Complaints Dept.	Quarterly
14			No of fraudulent transactions	0	FICM	Quarterly
15			No of cash shortfall incidents	0	Internal Audit Report	Quarterly

S. N.	Functional Area/Department		Indicators	Thresholds	Data Source	Frequency
16			No of procedural non-compliance identified in audit report per branch/department	<=5	Internal Audit Report	Quarterly
17			Non-compliance of internal audit/ control observations per branch	<=5	Internal Audit Report	Quarterly
18	Operational Risk	IT/MIS	No. of IT Audit	1	IT	Yearly
19			No. of pending AMC contracts for renewal	0	IT	Quarterly
20			No. of Server Audit	1	IT	Yearly
21			No. of System logs Audit	1	IT	Quarterly
22			No. of incidents system downtime	<=3	IT	Quarterly
23			Average length of system breakdown	<=2 hours	IT	Quarterly
24			No of user credential resets	<=10	IT	Quarterly
25			No. of pending unresolved tickets	<=3	IT	Quarterly
26	Regulatory/Legal Risk	Compliance	No. of financial penalties by regulator for non-compliance	0	Compliance	Quarterly
27			No. of regulatory citations /sanctions for non-compliance	0	Compliance	Quarterly
28			No. of business relationship and transactions with non-tax compliant suppliers	0	Compliance	Quarterly
29	Operational Risk	Administration	No. of instances of irregularities in purchases made by the Company	0	Internal Audit Report	Quarterly
30	Operational Risk	Finance & Accounting	No. of missed monthly closing deadlines	0	Finance & Accounting Dept.	Quarterly
31			No. of journal voucher reversals and adjustments	<=5	Finance & Accounting Dept.	Quarterly

5.2.6. Management-level Operational Risk Management Committee

The Company has instituted Management-level Operational Risk Management Committee. The purpose of the Committee is to assist the executives with respect to operational risk related matters, including overseeing: (a) the Company's risk management system that is commensurate with the Company's size, complexity and risk profile; and (b) the Company's Operational Risk Management framework and policies related to operational risks, (c) monitoring the Company's operational risk management and remediation plan; (d) holding discussions on emerging risks that may have impact on the Company and assessing mitigation wherever required. Committee's charter sets forth the authority and responsibility of the Committee in fulfilling its purpose.

5.3. Liquidity Risk

Liquidity risk is the risk that the Company may not be able to fund increases in assets (primarily loans) or meet obligations as they fall due, without incurring unacceptable losses.

This may be caused by the Company's inability to liquidate assets or to obtain funding to meet its liquidity needs.

Resource Planning Policy of the Company takes care of the long-term and short-term resource mobilization plans. It also has Contingency funding plan to address any unforeseen contingency of stressed liquidity.

Liquidity Risk Concentration

In order to reduce dependence on a single lender, the Company has adopted a cap on borrowing from any single lender at 25%. The Company intends to bring it down to 15% for all lenders, except SBI for which the limit shall be 25%.

6. RISK APPETITE FRAMEWORK

Risk Appetite can be defined as the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time within the context of its business strategy. Definition of an organization wide Risk Appetite Statement is an essential pre-requisite for developing a sound risk management framework.

The Risk Appetite Framework (RAF) provides a structured approach to the management, measurement, and control of risk, i.e., a way that people and processes ensure that business activities provide an appropriate balance of return for the risk assumed and remain within the stated risk appetite of the institution.

6.1. Risk Appetite Statement

The Risk Appetite statement defines the amount of risk that a Company is ready to be exposed to under various risk categories by way of establishing thresholds / limits. Risk appetite is either quantitatively defined by the appropriate indicators (e.g., capital adequacy level and risk limits) or qualitatively embedded in the group entities policies and procedures (e.g., underwriting criteria). Each entity's risk policy and risk limits are designed to be consistent with the defined risk appetite.

The Risk Appetite is guided by the strategies and goals of the Company. It is also dependent on the culture of the Company (conservative /aggressive) and the degree and quantum of availability of resources like capital, business skills, risk management skills, etc.

The Risk Appetite of the Company shall be determined for the various risk elements by the Board / senior management taking a holistic view of the Company's resources, its short and long-term strategies and objectives. While the Board / Board designated Committee specifies a broad level appetite for various risks, senior management and Business Line/ Operations Heads are just equally responsible for identifying detailed metrics to monitor the risk levels for different risk elements and to allocate the exposure limits to Business Lines.

Risk appetite also forms the basis for the calibration, setting of delegation and limits for all aspects of market, credit, liquidity and operational risk. The risk appetite statements address both quantitative and qualitative aspects of risk taking.

Qualitative risk appetite statements

- The Company shall ensure full compliance with regulatory requirements
- The Company shall ensure compliance to the organisation's vision, mission and organisational objectives and avoid situations/actions that could have negative impact on its reputation and brand
- The Company shall ensure compliance with operational risks in the execution of business plan
- The Company shall implement effective lending operating policies, and procedures, with appropriate internal controls
- The Company shall ensure development and adherence to Board approved concentration limits, and credit risk indicators

Quantitative risk appetite statements

- The Company shall maintain minimum external credit rating level of BBB or its equivalent rating.
- The Company shall maintain minimum regulatory capital at 15% of Risk Weighted Assets (RWAs) with Trigger level set at 20% of RWAs.
- The Company shall maintain minimum tolerance for market, credit and operational losses.
- Minimum excess liquidity resources to meet peak stressed liquidity requirements without the need to liquidate assets or raise capital.

Risk appetite indicators shall be monitored by the RMC by way of a risk dashboard. Risk indicators and limits for each risk category are mentioned in subsequent sections of the document.

6.2. Stakeholders in Risk Appetite Framework

To monitor and control the risk appetite of the Company, it has following stakeholders:

i. Board of Directors

The Board and the senior management of the Company communicate the business strategy and risk appetite to the business line teams as a means of providing clear direction to the business units for on-going operation and risk management. The Board of Directors is responsible for defining the Risk Appetite of the Company. The Board decides on the level and quantum of various risks that the Company can accept to carry on its business operations. The risk appetite is assessed regularly to check for any breaches. In the event of a breach, appropriate management action plans is drawn to bring down the exposures within the risk appetite set and strengthen the controls. The Board is guided by suggestions from the senior management, committees and departments. However, the final definition of Risk Appetite is made by the Board.

ii. Risk Management *Committee (RMC)*

The RMC is responsible to review the Risk Appetite Framework at least on an annual basis. It is also responsible to review the breaches in Risk Appetite and authorize the breach in limits. It also provides inputs to the Board for defining the Risk Appetite.

iii. Risk Management Department

The Risk Management Department is one of the main stakeholders in defining the Risk Appetite. Risk Management Department provides inputs for the risk limits and tolerances defined for the respective risk area in the Risk Appetite statement.

iv. Business Operations

The Business Operations are required to ensure that the business plans, activities are in line with the Company's Risk Appetite. They need to comply with the risk limits allocated to them and provide support in terms of data and information to understand the degree of compliance with the Risk Appetite.

v. Internal Audit

The audit exercise is a risk-based process where levels of inherent risks in the entity and the extent, adequacy and application of mitigating controls are accessed across certain defined risk parameters. The key responsibilities in the scope of RAF shall include:

- To independently review the function of Risk Management Department and ensure adherence to the laid down policies and procedures
- To independently review the adequacy and appropriateness of the risk measurement process

6.3. Risk Appetite Metrics

Company has defined its risk appetite for the major risk areas, viz. Credit Risk, Market Risk, Operational Risk, etc. For each of these risk areas, relevant metrics have been identified which are mostly operational working limits. These risk limits/metrics are monitored periodically keeping in mind the overall risk appetite of the Company. The appetite for risk has been defined in terms of these metrics.

7. STRESS TESTING FRAMEWORK

In any business environment, risks are unavoidable. The unexpected losses, however, are of particular importance while analysing the risks to the viability of business as normal. Stress Testing provides a tool to construct exceptional but plausible stress events and to analyse their impact on the profitability, capital and sustainability of the financial institution. Stress testing techniques provide a way to quantify the impact of changes in a number of risk factors on the assets and liabilities of the Company.

Stress Testing exercise provides signals to the management regarding adverse and unexpected outcome related to different risks and helps in indicating the Capital that shall be required to absorb losses if the assumed stress scenarios materialise. Accordingly, the organisation can plan appropriate mitigant strategy like, capital infusion or reducing the exposure, or transfer of risk, where warranted, etc. In essence, Stress Testing is a tool that supplements other Risk Management approaches and captures the impact of the unlikely but plausible events. The idea of the Stress test is to gauge the impact of adverse scenarios on the Company's Capital Adequacy Ratio (CRAR). CRAR gets impacted by the change in P&L as well as changes in Company's capital requirements.

RBI had issued Stress Testing Guidelines for the Scheduled Commercial Banks (excluding Regional Rural Banks) in 2013. In absence of any guidelines on Stress Testing for NBFC-

MFIs, the proposed stress testing framework has been designed to be commensurate with the nature, scope, scale and the degree of complexity in the Company's business operations and the risks associated with those operations.

7.1. Stress Testing exercise

Shocks have been proposed in Credit, Operational, Interest rate and Liquidity risk areas.

7.1.1.Credit Risk

Objective:

To assess the impact of macro-economic cycles as well as sector specific factors on company's financial performance-CRAR or profitability

Methodology:

- Shock 1: *Increase in NPAs*- Net NPA increase by 25 (Baseline), 50 (Medium), and 100 (Severe) percent, and simultaneous increase in provisioning to actual provisioning levels of the quarter over one-year period.
- Shock 2: *Increase in NPA in Top Five Sectors/Industries*- Additional 1 (Baseline), 2 (Medium) and 5 (Severe) percentage points increase in Net NPAs
- Shock 3: *Slippage of Restructured Standard Assets*- Additional slippages in restructured standard assets – 10 per cent (Baseline), 20 per cent (Medium) and 30 per cent (Severe) of restructured standard assets.
- Shock 4: *Default in Top States*- Default in 5% of the POS in States due to Pandemic/Political developments – Default in top one State (Baseline), top two States (Medium), top four States (Severe)

Assumptions:

- Stress testing shall be done on outstanding balance as on date.
- All the new NPA advances shall be categorized in Sub-standard accounts after defaults.
- NPA shall increase uniformly in sub-standard and Doubtful accounts.
- Overall provisioning levels shall remain same at the quarter-end levels.
- Same risk weights shall be used for stress testing as used for calculation for CRAR.

7.1.2.Operational Risk

Objective:

To assess the impact of general operational losses on company's financial performance-CRAR or profitability

Methodology:

Stress 1: Losses due to, e.g., penalty from regulators, cybercrime, IT breaches, fraud, litigation, natural disaster or any other adverse operational event during the quarter. Impact on NII at (i) 0.1x quarterly loss due to Loss events (Baseline) (ii) 0.2x of quarterly loss due to Loss events (Medium) and (iii) 0.3x of quarterly loss due to Loss events (Severe).

Stress 2: Losses due to Disruption in Business days [10 days (Baseline), 20 days (Medium) and 30 days (severe)] due to terror strike/natural calamities/employees' strike

Assumptions:

- General operational loss events (like, penalties, frauds, natural disasters, etc.) during the quarter shall form as the base level for creating stress scenarios.

7.1.3.Interest Rate Risk

Objective:

To analyse the impact of change in the interest rate on profitability.

Methodology:
Interest sensitive assets and liabilities shall be plotted as per maturity bucket based on the maturity period. The focus of analysis shall be on the impact of changes in interest rates on earnings. Variation in earnings is an important focal point for interest rate risk analysis because reduced earnings or outright losses can threaten the financial stability of an institution by undermining its capital adequacy and by reducing market confidence. The impact of this measure is usually over one year.
Interest rate shall be stressed by taking following three different scenarios:

- Increase in rate by 1 %
- Decrease in rate by 1%
- Increase in rate by 1% on assets and liabilities maturity up to 6 months and decrease in rate by 1% on assets and liabilities maturity beyond 6 months and up to 1 yr.

Impact of change in the rate shall be assessed on the profitability in all three scenarios.

Assumptions:
Where all assets are linked to floating interest rates and liabilities are fixed in nature, any change in the interest rates shall normally impact the interest rates pertaining to those assets which are due for maturity/ re-pricing within the time horizon over which the stress is envisaged. When there is a change in the Repo rate, the change shall impact the interest rates of all assets, including those that are due for re-pricing/ maturity beyond the time horizon over which the stress is envisaged.

*7.1.4.**Liquidity Risk***

Objective:
To analyse the impact on stress testing on liquidity profile of the Company.

Methodology:

- Components of assets and liabilities shall be plotted as per maturity and bucket wise mismatches shall be arrived at.
- Various stress situations shall be considered as mentioned in the assumptions to know the impact on liquidity.

Cost of above stress scenarios shall be assessed to determine impact on profitability.

Assumptions:

- Debt Securities: - 50% of these shall be repaid in the first bucket.
- Borrowings: - 20% of these, which mature beyond 30 days, shall mature in first two bucket in the ratio of 50:50.
- For meeting liquidity gap in first three buckets, Company may resort to borrowings from the market.

The above assumptions may undergo a change with changed circumstances.

The framework shall strive to assess stress scenarios from the credit risk, operational risk, interest rates risk and liquidity risk point of views that the Company foresees for itself. The exercise shall be conducted at quarterly interval and the results shall be presented to the Risk Management Committee (RMC).

As the environment in which the Company is operating is quite dynamic, the stress testing framework shall be reviewed periodically determine its efficacy and to consider the need for modifying any of the elements.

8. Conclusion

The Company has a well-established and strong internal control with well-designed systems, policies and procedures to maintain financial discipline. The Company's Internal Control Systems are commensurate with the nature of its business and the size and complexity of its operations. Based on the guidelines received on various issues of control from the Reserve Bank of India and the Government of India, the Company's Board of Directors and Risk Management Committee shall ensure compliance at all levels.

*****