PRAYATNA
MICROFINANCE
प्रयत्न योग्यता पहचान

PRAYATNA MICROFINANCE LIMITED

RISK MANAGEMENT POLICY

Prayatna Microfinance Limited New Delhi

Introduction

Risk in the context of business is defined as probability of liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities. While risk is inherent to every institution, it assumes greater significance in the context of microfinance due to the varying nature of the business and absence of collateral security or guarantee.

Further, Microfinance, by its nature, involves extending financial services to underserved and economically vulnerable segments of society. While this presents an opportunity to drive positive social impact and financial inclusion, it also exposes the company to unique risks that require careful management. These risks encompass a wide range of areas including credit risk, operational risk, market risk, liquidity risk, financial risk and regulatory risk.

Risks may be avoided through preemptive action and hence there is a need to identify the risks and put in place various mitigation mechanisms. Proactive risk management is essential to the long-term sustainability of microfinance institutions (MFIs). This document presents a framework for proactive risk management processes, internal risk management systems, tools for mitigation of various risks.

Prayatna Microfinance Limited ("Company" or "Prayatna") is registered with RBI, focused on providing financial support to women from low income households engaged in economic activity for income generation with limited access to financial services.

The Company has adopted this Risk Management Policy to set out the guidelines, principles and approach to manage risks for the Company and establish a risk mitigation culture and risk governance framework to enable identification, measurement, mitigation and reporting of risks within the Company. The Risk Management Policy of the Company aims to mitigate adverse effects on business objectives and safeguard stakeholders value.

Purpose

The purpose of the risk management policy is to provide guidance on identifying, managing and mitigating risks arising across risk taking activities in the organization to ensure sustainable business growth and profitability. This policy applies to activities and processes associated with the operations of the organization and covers areas such as credit risk, operational risk, market risk, liquidity risk, financial risk, regulatory risk and also covers business aspects related to reputation, technology, finance, regulatory, strategy, business continuity, data security etc.

This policy specifies Prayatna's commitment to prudently managing risks in the pursuit of its mission to empower individuals and communities through responsible microfinance. By staying vigilant, adaptive and proactive in the risk management approach, Prayatna seeks to navigate the challenges of the operating environment while maximizing opportunities for sustainable growth and social impact.

Principles

For risk management to be effective, all operations/departments of the Company must apply the following principles to the context of the business and its objectives:

- Risk management must create and protect value;
- Risk management is integrated into organizational processes;

- Explicit risk management helps decision-makers make informed choices;
- Risk management is focused on the sources of uncertainty around the achievement of objectives;
- Risk management must be tailored to the context and fit for purpose; and
- Risk management is dynamic, iterative and responsive to change.

Risk Management should consist the following basic building blocks:

- **Risk appetite and strategy:** Risk appetite clarifies the risks that the organisation is prepared to accept and manage in the pursuit of its objectives and those which it does not.

- **Organisation structure and governance:** Organisation structure and governance framework ensures independence of the risk function while providing sufficient oversight and effective challenge.

- **Credit risk assessment and risk analytics:** Analytics shall be embedded directly into making decisions, taking action and delivering value to various stakeholders. Analytics shall deliver agility and ensure test and learn on tools and models for developing holistic customer view.

- **Risk controls, monitoring and reporting:** Effective monitoring process with early warning signals and feedback mechanisms in policies shall be in place.

- **Risk culture:** Prayatna may strive to build and embed a common organisation culture with shared goals and objectives. The organisation shall focus on building a healthy risk culture by linking performance to risk and capital metrics.

Definitions

- **"Business unit"** is responsible for identifying and managing the risks inherent in the products, services, activities, processes and systems for which it is accountable and includes all associated support, corporate and/or shared service functions, e.g., Finance, Human Resources and Operations and Technology. It does not include Risk Management and Internal Audit functions.

- "**Critical operations**" refers to critical functions, activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of the Company or its role in the financial system. Whether a particular operation is "critical" depends on its role in the financial system.

- **"Event management"** is the process of identification, analysis, end-to-end management and reporting of an operational risk event that follows a pre-determined set of protocols.

- "**Incidents**" are current or past disruptive events the occurrence of which would have an adverse effect on critical operations of the Company. Incident management is the process of identifying, analysing, rectifying and learning from an incident (including a cyber-incident) and preventing recurrences or mitigating the severity thereof. The goal of incident management is to limit the disruption and restore critical operations in line with the Company's risk tolerance for disruption.

Prayatna Microfinance Limited New Delhi

- "**Information and Communication Technology**" refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environment.

- "**Mapping**" is the process of identifying, documenting and understanding the chain of activities involved in delivering critical operations. It incorporates the identification of all interdependencies and interconnections including people, processes, technology and third parties.

- "**Operational resilience**" means the ability of a Company to deliver critical operations through disruption. This ability enables the Company to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events to minimise their impact on the delivery of critical operations through disruption.

- "**Operational Risk**" means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. It includes legal risk but excludes strategic and reputational risk and it is inherent in all financial products, activities, processes and systems.

- "**Operational Risk Management**" refers to entire gamut of activities right from risk identification, measurement and assessment, monitoring and control, mitigation, reporting to senior management and the Board of Directors on the Company's risk exposures, Business Continuity Management and learning through feedback for improvement.

- "**Operational Risk profiles**" describe the Operational Risk exposures and control environment assessments of business units of Company's and it considers the range of potential impacts that could arise from estimates of expected to plausible severe losses.

- "**Respective functions**" refers to the appropriate function(s) within the Company's three lines of defence, which are (i) business unit management; (ii) an independent Operational Risk Management including Compliance function; and (iii) audit function.

- "**Risk appetite**" is the aggregate level and types of risk the Company is willing to assume, decided in advance and within its risk capacity, to achieve its strategic objectives and business plan.

- "**Risk tolerance**" is the variation around the prescribed risk appetite that the Company is willing to tolerate.

- "**Supervisory Authority**" means, Reserve Bank of India (RBI).

- "**Tolerance for disruption or Impact Tolerance**" is the level of disruption from any type of Operational Risk the Company is willing to accept given a range of severe but plausible scenarios.

Policy

Company has identified the following potential risks that could have an adverse impact on the company:

1) Credit Risk (including New to Credit Client Risks)
2) Operational Risk
3) Liquidity Risk

Navatna Microfinance Limited New Delhi

4) Portfolio Concentration Risk
5) Reputation Risk
6) Strategic Risk
7) Regulatory and Compliance Risk
8) Geographical Risk

CREDIT RISK

Credit Risk for Prayatna is the risk of loss of interest income and the Company's inability to recover the principal amount of the loan disbursed to its customers.

This risk can result from:

- Information asymmetry and excessive reliance on Credit Bureau check, not backed by reliable information or market intelligence on a territory or group of borrowers, leading to adverse selection of borrowers.
- A volatile political presence in a region of exposure.
- Exposure to activities with a high probability of variation in earnings.
- Default due to over-indebtedness or income generation activity failure.

Credit Risk also includes Credit Concentration Risk, arising out of concentrated exposure to a particular geographical location/territory or to an activity in which a large group of borrowers are engaged in, vulnerable to external events.

New-to-credit borrowers, which pertains to individuals with no prior credit history who have recently obtained their first-ever credit from the Company. The inherent risk is associated with extending loans to such borrowers due to the lack of credit bureau information available to the Company.

MITIGATION OF CREDIT RISK

1. Location Selection

Before establishing any branch, a detailed survey should be conducted which takes into account the following factors:

- **Credit Culture:** To see if there is a history of a good credit culture and some level of financial literacy.
- **Economic Activity:** To see if it is in an economically active area not overly dependent on seasonal demands or on monsoons, etc.
- **Political Stability:** To see if there is any history of local political influence on micro finance activities.

This mitigates the risk of operating in expected negative areas.

2. Credit Bureau Check

A credit check is done for every customer through an automated system-to-system integration with the Credit Bureau. As part of this check, the following parameters are looked at to verify a customer's credit-worthiness and also ensure that they are not overburdened.

- **Default History:** Only those customers who have no default or write-off at that time are approved.
- **Multiple Borrowings:** Only those customers who do not have more than one existing MFI loan are approved.

Prayatna Micro Finance Limited New Delhi

- **Indebtedness:** Only those customers whose total loan outstanding under JLG/SHG including our proposed loan amount will be lesser prescribed limit are approved. These will be dynamic and reviewed periodically based on RBI Regulations, MFIN and Sa-Dhan Directives and Company's Internal Norms.

This mitigates the risk of customer defaults.

OPERATIONAL RISK

Operational risk is quite a complex risk to handle. Pinpointing its extent, measuring it, and finding ways to minimize is tricky. This type of risk is influenced by many factors such as how our business operates internally, the rules and regulations we must adhere to, company's growth trajectory, customer preferences, and external factors beyond our control. It's a dynamic risk because it's constantly evolving with the introduction of new elements like cutting-edge technologies, data accessibility, latest rules and regulations, and collaborations with external parties.

Being a microfinance entity, Prayatna engages with various third parties, be its lenders or clients. It is imperative for the company to consider and address any supplementary risks emerging from other areas. These risks could potentially impact the company's capability to manage a significant disruption to its operations effectively. Therefore, Prayatna shall be vigilant in recognizing and addressing risks associated with any third party. This ensures a comprehensive understanding of the extended chain and potential issues that could jeopardize the entity's ability to sustain its critical operations.

Operational Risk Management and resilience

Operational Risk Management enables an organization to more effectively recognize, evaluate and eleminate operational risks, on the other hand, Operational Resilience empowers the organization to maintain essential functions even in the face of disruptions. While Operational Risk Management and Operational Resilience pursue distinct objectives, they are intricately linked. A well-functioning Operational Risk Management framework and a resilient Operational Resilience system collaborate to decrease the occurrence and severity of operational risk incidents.

Further, with the introduction of "Guidance Note on Operational Risk Management and Operational Resilience" dated 30th April, 2024 by RBI prepared based on the Basel Committee on Banking Supervision (BCBS) principles which is now applicable on all regulated entities including NBFCs, Operational Risk Management and resilience has been further elaborated to inter alia cover man-made causes, Information Technology (IT) threats (e.g., cyber-attacks, changes in technology, technology failures, etc), geopolitical conflicts, business disruptions, internal/external frauds, execution/ delivery errors, third party dependencies, or natural causes (e.g., climate change, pandemic, etc.). As per the said guidance note, Operational Risk Management refers to entire gamut of activities right from risk identification, measurement and assessment, monitoring and control, mitigation, reporting to senior management and the Board of Directors on the Company's risk exposures, Business Continuity Management and learning through feedback for improvement.

Operational resilience refers to the ability of the organization to maintain essential functions and operations, even in the face of various disruptions or challenges. This includes the capacity to withstand and recover from unexpected events such as natural disasters, technological failures, regulatory changes, economic downturns or other operational disturbances.

For Prayatna, operational resilience involves ensuring that its core functions, such as providing financial services to underserved communities, managing loan portfolios, collecting

repayments, and maintaining regulatory compliance, remain robust and uninterrupted despite adverse circumstances. This may entail implementing contingency plans, diversifying risk, adopting resilient technology systems, establishing effective communication channels, and having well-trained staff to respond effectively to crises.

Further, as per the said guidance note "**Operational resilience**" means the ability of a Company to deliver critical operations through disruption. This ability enables the Company to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events to minimise their impact on the delivery of critical operations through disruption.

The said guidance note had elaborated and suggested that Risk Management and Operational Resilience have been built on three pillars. The three pillars are:

(i) Prepare and Protect

- Business Unit Management (First Line of Defence)
- Organisational Operational Risk Management Function including Compliance Function (Second Line of Defence)
- Audit Function (Third Line of Defence)

(ii) Build Resilience

- Developing an independent view regarding business units' (a) identified material Operational Risks, (b) design and effectiveness of key controls, and (c) risk tolerance;
- Challenging the relevance and consistency of the business unit's implementation of the Operational Risk Management tools, measurement activities and reporting systems, and providing evidence of this effective challenge;
- Developing and maintaining Operational Risk Management and measurement policies, standards and guidelines;
- Reviewing and contributing to the monitoring and reporting of the Operational Risk profile; and
- Designing and providing Operational Risk training and instilling risk awareness
- Operational Compliance

The above functions of both first and second line of defense can be carried out by the same unit for smaller regulated entities like us and independence may be achieved through separation of duties within the same unit by the same or different persons.

(iii) Learn and Adapt

The third line of defense, i.e. the audit function provides an independent assurance to the Company regarding the appropriateness of operations. This function's staff should not be involved in the development, implementation and operation of Operational Risk Management processes which has been carried out by the other two lines of defence. The third line of defence reviews are generally carried out by Company's internal and/or external auditor but may also involve suitably qualified independent third parties, if required. The scope and frequency of reviews should not only be sufficient to cover all activities aligned with the Company Operational Risk profile and identify and prioritize key risk areas that warrant thorough examination but also be responsive to the dynamic nature of the Operational Risk environment. An effective independent review includes two processes:

a) Validation
b) Verification

Prayatna Microfinance Limited New Delhi

"Guidance Note on Operational Risk Management and Operational Resilience" dated 30th April, 2024 by RBI, has further suggested comprehensive mechanism for Operational Risk Management and Operational Resilience, which is considered by the Company to refer to the extent possible whenever required. The said guidance note has specified three pillars with 17 principles for Operational Risk Management and Operational Resilience. The said pillars and principles have been summarized below and may be referred by the Company as and when required according to the circumstances to mitigate the operational risk and resilience.

PILLAR 1: Prepare and Protect

➢ GOVERNANCE AND RISK CULTURE

Principle 1- The Board of Directors should take the lead in establishing a strong risk management culture, implemented by Senior Management. The Board of Directors and Senior Management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behavior, and ensure that staff receives appropriate risk management and ethics training.

Prayatna has already put in place employee's code of conduct which is applicable on employees but as guided by the said guidance note it is now applicable on senior management and Board also. Prayatna has previously implemented HR Policy containing employee compensation, incentive/bonus, promotion etc. Further, Company has put in place required hierarchy of the employees as well as training module in place.

Principle 2- Company should develop, implement and maintain an Organisation Risk Management Framework (ORMF) that is fully integrated into the Company's overall risk management processes. The ORMF adopted by Company will depend on a range of factors, including its nature, size, complexity and risk profile. Further, Company should utilize their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimize their impact on delivering critical operations through disruption.

The Company has assessed nature and complexities of the risk inherent in the business, products, services, activities, process and systems. These all risk areas are governed/headed by various operation department heads who are independent to the risk assessment and audit team.

The Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhering to apply the ORMF, when Company would grow and become of the reasonable size. The Company identify that the proposed ORMF documentation should clearly:

- identify the governance structures used to manage Operational Risk, including reporting lines and accountabilities, and the mandates and membership of the Operational Risk governance committees;
- reference the relevant Operational Risk Management policies and procedures;
- describe the tools for risk and control identification and assessment and the role and responsibilities of the three lines of defence in using them;
- describe the Company's accepted Operational Risk appetite and tolerance; the thresholds, material activity triggers or limits for inherent and residual risk and the approved risk mitigation strategies and instruments;
- describe the Company's approach to ensure controls are designed, implemented and operate effectively;

Prayatna Microfinance Limited New Delhi

- describe the Company's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;
- describe inventory risks and controls implemented by all business units (e.g., in a control library);
- establish risk reporting and management information systems (MIS) for producing timely, and accurate data;
- provide for a common taxonomy of Operational Risk terms to ensure consistency of risk identification, exposure rating and risk management objectives across all business units. The taxonomy can distinguish Operational Risk exposures by event types, causes, materiality and business units where they occur; it can also flag those operational risk exposures that partially or entirely represent legal, conduct, model and ICT (including cyber) risks as well as exposures in the credit or market risk boundary;
- provide for appropriate independent review and challenge of the outcomes of the risk management process; and
- require the policies to be reviewed and revised as appropriate based on continued assessment of the quality of the control environment addressing internal and external environmental changes or whenever a material change in the Operational Risk profile.

➢ RESPONSIBILITIES OF BOARD OF DIRECTORS AND SENIOR MANAGEMENT

Principle 3- The Board of Directors should approve and periodically review the ORMF and Operational Resilience approach, and ensure that Senior Management implements the policies, processes and systems of the ORMF and Operational Resilience approach effectively at all decision levels.

The Board of Directors should:

- establish a risk management culture and ensure that the Company has adequate processes for understanding the nature and scope of the Operational Risk inherent in its current and planned strategies and activities;
- ensure that the Operational Risk Management processes are subject to comprehensive and dynamic oversight and are fully integrated into, or coordinated with, the overall framework for managing all risks across the enterprise;
- provide senior management with clear guidance regarding the principles underlying the ORMF, and approve the corresponding policies developed by senior management to align with these principles;
- regularly review and evaluate the effectiveness of, and approve the ORMF to ensure the Company has identified and is managing the Operational Risk arising from external market changes and other environmental factors, as well as those Operational Risks associated with new products, services, activities, processes or systems, including changes in risk profiles and priorities (e.g. changing business volumes);
- ensure that the Company's ORMF is subject to effective independent review by a third line of defense (audit or other appropriately trained independent third parties from external sources); and
- ensure that, as best practices evolve, management is availing themselves of these advances.

Principle 4- The Board of Directors should approve and periodically review a risk appetite and tolerance statement for Operational Risk that articulates the nature, types and levels of Operational Risk the Reporting Entity (RE) i.e. Prayatna is willing to assume. The Board of Directors should also review and approve the criteria for

Prayatna Microfinance Limited New Delhi

identification and classification as critical operations as well as of impact tolerances for each critical operation, in order to enhance Company's Operational Resilience.

The Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhere to apply the ORMF, when Company would grow and become of the reasonable size and once the ORMF would applicable the above said Principle 4 would also be applicable.

Principle 5- Senior Management should develop for approval by the Board of Directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior Management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing Operational Risk in all of the Company's material products, activities, processes and systems consistent with its risk appetite and tolerance statement.

The Company has already put in place a well defined job profile for each and every profile including senior management. Further, Company also has various Committee's with well defined operation areas and structure of the Committees including Risk Management Committee, structure of which is described below:

S. No.	Board/Management	Designation
1.	Managing Director	Member
2.	Whole Time Director	Member
3.	CFO	Member

➢ RISK MANAGEMENT ENVIRONMENT - IDENTIFICATION AND ASSESSMENT

Principle 6- Senior Management should ensure the comprehensive identification and assessment of the Operational Risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Both internal and external threats and potential failures in people, processes and systems should be assessed promptly and on an ongoing basis. Assessment of vulnerabilities in critical operations should be done in a proactive and prompt manner. All the resulting risks should be managed in accordance with operational resilience approach.

Following areas of operational risk with mitigation thereof has been identified and already incremented by the Company:

- **Document Storage and Retrieval:** Prayatna recognizes the need for proper storage of documents and also their retrieval for audit and statutory requirements. The Company is maintaining all the original documents in a fire proof vault at a dedicated space allocated for specific purpose.

- **Whistle Blower/Fraud Prevention Policy:** Prayatna encourages all its employees to report any non-compliance of stated company processes or policies without fear as we have a clearly stated "no-retaliation" policy. All issues reported are categorized for nature and severity:

Prayatna Microfinance Limited New Delhi

- Financial or Non-Financial
- Major or Minor
- Procedural Lapse or Gross Violation
- Breach in Process or Disciplinary Issue

The Compliance Manager maintains a record of all the entire case history which is signed off by senior management on closure.

- **Employee Rotation Policy:** We have a policy to ensure that no field employee is posted in the same location for over two years as an effort to mitigate any chances of collusion or fraud. All field employees are either transferred to another branch or rotated to another role in a programmed manner so as to mitigate the chances of collusion with other employees or customers. The policy ensures that the employees have the predictability of their movements without putting them into undue hardships. The company takes care of any additional expenses incurred on transfer to non-home base locations.

- **Internal Audit:** Internal Audit at Branch Offices and at the Corporate/Regional Offices shall be carried out on half yearly basis by an independent audit firm appointed by the Board. The scope of this Internal Audit covers all key functions including HR, Operations, Credit, Administration, Finance and Accounts. The firm also audits the company's adherence to all Statutory and Regulatory Guidelines that have been prescribed for NBFC-MFIs. The scope of these audits are reviewed periodically and modified to keep pace with a dynamic business environment. All significant audit observations of Internal Audits and follow-up actions are presented to the Board.

- **Technology Infrastructure:** The company has leverage of cloud-based technologies and all its business applications are hosted in secure data centers with mirrored redundancies such that in the event of any system going down, an alternate system is made operational within hours. At the facilities where back-office and financial operations take place, alternate/back-up connectivity has been provisioned such that in the event connectivity is lost with one service provider, the alternate connection can be utilized.

- **Losses and near misses:** Some events lead to a financial loss or a gain; other events do not lead to a financial impact. Operational risk events that do not lead to a loss or gain are called "near misses". In other words, near miss is a risk event where failed or inadequate internal processes, people, system, or external event occurred but it did not result in a direct or indirect impact on the organization. Recording of near miss events gives important information for risk management purposes.

- **Compliance and Regulatory Oversight:** Maintaining strict adherence to regulatory requirements and compliance standards relevant to microfinance operations. Regular audits and assessments can help identify and address operational risks associated with non-compliance.

Prayatna Microfinance Limited New Delhi

- **Training and Capacity Building:** Prayatna provides regular training and capacity-building programs for staff to enhance their awareness of operational risks and equip them with the skills to identify and respond to potential risks effectively.

The above stated areas of operational risk are indicative and not exhausted, Company will time to time assess and mitigate the risk whenever an event would occur applying the mitigation tools available with the company.

➢ CHANGE MANAGEMENT

Principle 7- Senior Management should ensure that the Company's change management process is comprehensive, appropriately resourced and adequately articulated between the relevant lines of defence.

The change of senior management of the Company does occur on exceptional basis. Whenever it would happen the Company ensures that the change over process will be comprehensive, appropriately resourced and adequately articulated and governed by the management of the Company.

➢ Monitoring and Reporting

Principle 8- Senior Management should implement a process to regularly monitor Operational Risk profiles and material operational exposures. Appropriate reporting mechanisms should be in place at the Board of Directors, Senior Management, and business unit levels to support proactive management of Operational Risk.

The Company has already implemented Finpage software which is one of the best in MFI industry; the said software provides various kinds of reports including operational risk reports like arrear report, NPA report, centre meeting report etc. The Company had also put in place HR One software which provided comprehensive, monitoring and reporting in respect of all the employees of the Company. The Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full in full. The Company is adhere to apply more monitoring and reporting measures, when Company would grow and become of the reasonable size.

➢ CONTROL AND MITIGATION

Principle 9- Company should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

The Company has well in place internal audit team equipped with required software and other tools. Further, the Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhering to apply more control and mitigation measures, when Company would grow and become of the reasonable size.

PILLAR 2: Build Resilience

➢ MAPPING OF INTERCONNECTIONS AND INTERDEPENDENCIES

Prayatna Microfinance Limited New Delhi

Principle 10- Once the Company has identified its critical operations, it should map the internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

The Company has reasonably identified interconnection and interdependencies of the critical operations. Further, the Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhere to put in place a process of mapping internal and external interconnections and interdependencies, when Company would grow and become of the reasonable size.

- **THIRD-PARTY DEPENDENCY MANAGEMENT**

Principle 11- Company should manage their dependencies on relationships, including those of, but not limited to, third parties (which include intra group entities), for the delivery of critical operations.

The Company has reasonably identified dependencies on relationships with third parties and intra group entities, if any. Further, the Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhere to put in place a process of mapping internal and external interconnections and interdependencies, when Company would grow and become of the reasonable size.

- **BUSINESS CONTINUITY PLANNING AND TESTING**

Principle 12- Company should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Business continuity plans should be linked to the Company's ORMF. Company should conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

- **INCIDENT MANAGEMENT**

Principle 13- Company should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations in line with the Company's risk appetite and tolerance for disruption. Company should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

- **INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) INCLUDING CYBER SECURITY**

Principle 14- Company should implement a robust Information and Communication Technology (ICT) risk management programme in alignment with their ORMF and ensure a resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the Company's critical operations.

The Company has already implemented Information Technology (IT) Policy contain IT risk assessment and management tools. Further, the Company is smaller in size as

Prayatna Microfinance Limited New Delhi

compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhere to adopt more measures, when Company would grow and become of the reasonable size.

Pillar 3: Learn and Adapt

- **DISCLOSURE AND REPORTING**

Principle 15- Company's public disclosures should allow stakeholders to assess its approach to Operational Risk management and its Operational Risk exposure.

The Company is smaller in size as compared to other regulated entities on which the said guidance note is applicable in full. The Company is adhere to adopt more measures, when Company would grow and become of the reasonable size. Even though Company is adhere to disclose and report every compliance which is applicable to the Company, to the public (wherever applicable) and to every applicable regulator and stakeholder.

- **LESSONS LEARNED EXERCISE AND ADAPTING**

Principle 16- A lessons learned exercise should be conducted after a disruption to a critical or important business service to enhance the Company's capabilities to adapt and respond to future operational events.

The Company would conduct a 'lessons learned exercise', including Root Cause Analysis, after any disruption to a business service with emphasis on critical service. This would include any potential material disruption to a third-party provider (including but not limited to a group entity, if any) that feeds into the delivery of a critical business service. The Company would utilise the information gathered as part of the incident management and disaster recovery process. The decisions and recovery processes determined would be used throughout the incident management process. This exercise would also be necessary to identify the matter of priorities in case of disruption as well as to define effective remediation measures to address deficiencies and failures to avoid discontinuity and service.

- **CONTINUOUS IMPROVEMENT THROUGH FEEDBACK SYSTEMS**

Principle 17- Company should promote an effective culture of learning and continuous improvement as operational resilience evolves through effective feedback systems.

As any other prudent business entity, Prayatna is also have approach of continuous improvement and learned from its own experiences, we will continue to do so and will improve our self from every experience. Prayatna is adhere for time to time up gradation of technology and other infrastructure, robust feedback system to ensure a continuous positive feedback, implementation of feedback received wherever required. Prayatna would ensure that through feedback we would maintain optimal operational resilience.

LIQUIDITY RISK

Liquidity Risk arises largely due to maturity mismatch associated with assets and liabilities of the company. Liquidity risk stems from the inability of the company to fund increase in assets, manage unplanned changes in funding sources and meet financial commitments when required. This could arise due to a range of reasons such as mismatch in the tenor of loan and funding

Prayatna Microfinance Ltd. New Delhi

sources, negative changes in the credit rating, market-wide liquidity event, delay in collections etc. Due to the high reliance on external sources of funds, Prayatna is exposed to various funding and liquidity risks comprising:

- **Funding Concentration Risk:** Concentration of a single source of funds exposes the Company to an inability to raise funds in a planned and timely manner and resort to high cost emergency sources of funds. Further, concentration of funding sources can also result in a skewed maturity profile of liabilities and resultant Asset-Liability mismatch.
- **Asset-Liability Mismatch:** A skewed asset-liability profile can lead to severe liquidity shortfall and result in significantly higher costs of funds; especially so during times of crises.
- **Interest Rate risk:** Interest Rate risk comprises the risk of increase in cost of funds due to an overall increase in the interest rates economy as well as sharp movements in interest rates across maturity profiles of the liabilities.
- **Market Perception Risk:** Due to inherent industry characteristics, the Company is exposed to perception risks, which can lead to decline in ability of a lender to increase exposure to the Microfinance sector and result lack of adequate and timely inflow of funds.
- **Leverage Risk:** A high degree of leverage can severely impact the liquidity profile of the company and lead to default in meeting its liabilities.

MITIGATION OF LIQUIDITY RISK

The key liquidity management policies being followed at Prayatna include:

- Rolling Short Term Liquidity Forecasts: This is done to identify any short term liquidity gaps and thereby take immediate corrective actions to bridge the same.
- Maintaining detailed estimates of projected cash inflows and outflows for the next few weeks or months so that net cash requirements can be identified.
- Maintaining investment accounts that can be easily liquidated into cash, or lines of credit with local banks to meet unexpected needs.
- Anticipating the potential cash requirements of new product introductions or seasonal variations in deposits or withdrawals
- Regular stress testing / scenario analysis to determine sufficiency of liquid assets to meet stressful situations.
- Meeting of Asset Liability Committee (ALCO) are held at regular intervals in order to effectively monitor any mismatch of Assets and Liabilities.
- **Building Relationships with Stakeholders:** Establishing strong relationships with stakeholders, including lenders, investors, and regulators, to enhance access to funding and liquidity support during periods of financial stress or market disruptions.
- **Maintaining Adequate Liquidity Reserves:** Holding sufficient liquid assets, such as cash, cash equivalents, and highly liquid investments, to cover short-term funding needs and unexpected cash outflows.

PORTFOLIO CONCENTRATION RISK

Portfolio concentration risk refers to the potential vulnerability arising from a high level of exposure to a particular segment, geographic area, or type of borrower within the microfinance

portfolio. This concentration risk can have adverse effects on the financial stability and sustainability.

Prayatna may be exposed to various Portfolio concentration risks comprising:

- **Segment Concentration**: Dependence on a specific group of borrowers, whether they are small business proprietors, farmers, or female entrepreneurs, can expose the company vulnerable to risks inherent to that particular sector. These risks might include economic downturns or alterations in governmental policies affecting that segment.
- **Geographic Concentration**: Heavy reliance on borrowers from a particular geographic area or region can expose the company to local economic conditions, political instability, or natural disasters that may disproportionately impact that area.
- **Counterparty Concentration**: Dependency on a limited number of funding sources, counterparties, or investors for financing can expose the company to risks related to the creditworthiness or liquidity of those counterparties.

MITIGATION OF PORTFOLIO CONCENTRATION RISK

Prayatna intends to maintain a diversified exposure in advances across various states to minimize concentration risk and mitigate the impact of economic downturns on repayment rates. The Company had also adopted a policy which limits the exposure in every state in which Company operates.

REPUTATION RISK

Reputation risk is the risk to earnings and capital arising from adverse perception of the image of the company, on the part of customers, counterparties shareholders, investors and regulators. It refers to the potential adverse effects, which can arise from the company's reputation getting tarnished due to factors such as unethical practices, regulatory actions, customer dissatisfaction and complaints leading to negative publicity.

The reputation of the Company may suffer as a result of its failure to comply with laws, regulations, rules, reporting requirements, standards and codes of conduct applicable to its activities, rather than compliance with the internal limits or procedure.

Presence in a regulated and socially sensitive industry can result in significant impact on Prayatna's reputation and brand equity as perceived by multiple entities like the RBI, Central/State/Local authorities, banking industry and last but not least, Prayatna's customers. The risk can emanate from:

- Political activism
- Non-Compliance with Regulations
- Customer Dissatisfaction

MITIGATION OF REPUTATION RISK

Prayatna has adopted proactive measures to minimize the risk of losing reputation such as sound risk management framework, good corporate governance, high level ethics and integrity, anti money laundering procedures, good business

Considering the vulnerability of our customer segment and the potential for negative political activism to affect the reputation of the company, we have in place

Prayatna Microfinance Limited New Delhi

- **Strict Adherence to Fair Practices Code:** All employees are trained and instructed to follow fair practices in all their dealings
- **Grievance Redressal Mechanism:** The company has a defined GRM is place and the same is communicated to all customers with the toll-free number.
- **Delinquency Management**: The Company does not resort to any coercive recovery practices and has an approved delinquency management policy including restructuring of loans where necessary.

STRATEGIC RISK

Strategic risk refers to the potential threats and vulnerabilities arising from the company's strategic decisions, actions or lack thereof, which may impact its long-term objectives, competitiveness and sustainability.

It is the risk to earnings and capital arising from lack of responsiveness to changes in the business environment and/or adverse business decisions, besides adoption of wrong strategies and choices.

MITIGATION OF STRATEGIC RISK

This is being addressed and the risk mitigated to a great extent, by referring matters of strategic importance to the Board, consisting of members with diversified experience in the respective fields, for intense deliberations, so as to derive the benefit of collective wisdom.

REGULATORY AND COMPLIANCE RISK

The company is exposed to risk attached to various statutes and regulations. Prayatna is present in an industry where the Company has to ensure compliance with regulatory and statutory requirements. Non- Compliance can result in stringent actions and penalties from the Regulator and/or Statutory Authorities and which also poses a risk to Company's reputation. These risks can be:

- Non-Compliance with RBI Regulations;
- Non-Compliance with other Statutory Regulations; and
- Non-Compliance with covenants laid down by Lenders.

MITIGATION OF REGULATORY AND COMPLIANCE RISK

Prayatna intends to comply with all the applicable compliances within time in order to be a fully compliant entity, further, internal audit are also conducted on compliance function wherein all regulatory compliances are reviewed.

GEOGRAPHICAL RISK

Geographical risk for Prayatna is the potential challenges and vulnerabilities associated with operating in specific geographic regions. These risks can stem from various factors, including:

- **Political Stability**: Operating in regions with political instability or frequent changes in government can expose the company to uncertainties in regulations, policies, and governance, impacting its operations and financial stability.
- **Economic Conditions**: Geographical areas with volatile economies, high inflation rates, unemployment, or dependency on a single industry can pose risks to the financial health of the company, affecting repayment rates and profitability.

- **Legal and Regulatory Environment**: Different regions may have varying legal frameworks and regulatory environments governing microfinance operations. Compliance with these regulations, licenses, and permits may differ, impacting the ease of doing business and overall risk exposure.
- **Social and Cultural Factors**: Socio-cultural dynamics such as language barriers, societal attitudes towards debt, gender roles, and local customs can influence the acceptance and success of microfinance initiatives. Understanding and navigating these factors are crucial for effective operations.

  Infrastructure: Access to reliable infrastructure, including transportation networks, communication systems, and banking facilities, is essential for the efficient functioning of the company. Operating in remote or poorly connected areas can increase operational costs and hinder service delivery.

MITIGATION OF GEOGRAPHICAL RISK

Mitigating geographical risks involves a combination of proactive strategies aimed at understanding, managing, and minimizing the impact of risks associated with operating in specific geographic regions. Here are several approaches adopted by the company to mitigate geographical risks:

- Credit Risk Management: Implementation of robust credit risk management practices, including thorough borrower assessment, credit scoring models, and repayment monitoring mechanisms. Regularly reviewing and adjusting credit policies based on evolving market conditions and risk profiles.
- Avoidance of Compliance and Regulatory Oversight: Staying abreast of regulatory requirements and compliance obligations in each geographic jurisdiction where we operate.
- Training and Capacity Building: Investing in training and capacity building initiatives for staff members operating in high-risk areas. Providing them education and resources to enhance their understanding of local contexts, risk factors, and best practices for risk mitigation.
- Customer Education and Support: Educating the borrowers about financial literacy, risk management, and responsible borrowing practices.

Policy Review and Approval

The Policy would be reviewed at the discretion of the Board of Directors. However, the policy can be reviewed at short notice depending on the exigencies/extraordinary situations, which may emanate during the course of Company's business. Such extraordinary situations may include significant changes in Government/Reserve Bank of India policies, global/national economic conditions, financial performance, etc. This Policy shall remain in force till the next revision is carried out and disseminated.

****

Prayatna Microfinance Limited New Delhi