Risk Management Policy

Digamber Capfin Limited

Document Control Page

Document Name	:	**Digamber Capfin Limited – Risk Management Policy**

Document Owner	**:**	**Compliance Department-Digamber Capfin Limited**
Reviewed By	**:**	**Board of Directors**
Approved By	**:**	**Board of Directors**

Classification	**:**	**Internal Use Only**
Distribution List	**:**	**Digamber Capfin Limited**

Revision History	
Dates	**Status**
24.08.2018	**Approved**
24.08.2019	**Reviewed**
05.09.2020	**Reviewed**
24.08.2021	**Reviewed**
26.05.2022	**Reviewed**
09.02.2024	**Amended**
07.05.2024	**Amended**
20.07.2024	**Amended**
21.07.2025	**Amended**

Table of Contents

Chapter

1

CHAPTER 1: INTRODUCTION AND OBJECTIVES OF RISK MANAGEMENT POLICY

1. Introduction

Digamber Capfin Limited (DCL) is registered as a Non-Banking Financial Institution under section 45 I A of the Reserve Bank of India (RBI) Act, 1934. As per the registration granted to DCL it is currently classified as a Non-Banking Finance Company-Micro Finance Institution under Middle Layer.

DCL has adopted the Joint Liability Group (JLG) Model for its Micro Finance Business and is also providing Individual Micro Loans (IML). The company is running its operations in various states of the country and its operations are being undertaken with a mix of manual as well as technology based efforts.

Financial services business esp. Micro finance Business involves various types of risks like (included but not limited to): -

- Strategic risk,
- Operational risk (Including technology risk),
- Financial risks (including liquidity & credit risk),
- Compliance/ Regulatory & Legal risk,
- Reputational risk,
- Investment risk,
- Interest Rate risk,
- Market risk,
- Concentration Risk
- Currency Risk
- Conduct Risk
- Human Capital Risk
- Outsourcing Risk
- Settlement Risk

- Model Risk
- IT Risk
- Physical Risk
- Other Risks as may be identified from time to time

If the above risks are not managed and mitigated properly, this may lead to disruption in business and impact the attainment of main objectives of the organization. Risk management works towards identifying and managing threats that could adversely impact the organization. This involves reviewing operations, processes & procedures of the organization, identifying potential threats and likelihood of their occurrence, and taking appropriate actions to address the most likely threats.

Primary objective of risk management is to ensure that the enterprise's asset and liability profile, its trading exposures and its operational & business activities do not expose it to losses that threaten the viability of the enterprise. In all circumstances, all activities giving rise to risk must be identified, measured, managed, mitigated and monitored.

Risk Management is a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Hence this policy covers risk management which includes risk assessment, mitigation and continuous review of the same.

2. Objectives of policy

The main objective of the policy is to keep the Board of Directors, Risk Management Committee and Top Management appraised of the applicable risks promptly and regularly.

This risk management policy aims, among other things, to protect the reputation of the organization, enable the Company to make consistently profitable and prudent business decisions across all its offices and ensure an acceptable risk-adjusted return on capital, Risk-Appetite based Risk-Tolerances (including defined Risk Limits as applicable) and to be within its overall risk capacity or any other equivalent measure.

In a nutshell it seeks to ensure growth with profitability within the limits of risk absorption capacity. The objectives can be shortlisted as under:-

1. Establish methodologies for identification, measurement and management of risk.
2. To build profitable and sustainable business with conservative risk management approach.
3. To have risk management as an integral part of the organization's business strategy.
4. To manage the risks proactively across the organization.
5. To develop a strong risk culture across the organization.

Chapter

2

CHAPTER 2: RISK GOVERNANCE FRAMEWORK & REPORTING

Effective implementation of the risk management would require active participation from all the stakeholders. The role and responsibility of various stake holders is listed below:

(i) Role of the Board of Directors

The primary role of the Board will be to risk oversight of management and corporate issues that affect Risk. The Board can fulfil the role of Risk Oversight by:

- Developing Policy and Procedures around risk that are consistent with the organization's strategy and risk appetite.
- Developing and implementing controls against Fraud Risk.

Risk Appetite: Risk appetite is the Company's capacity to bear risk and its attitude towards risk. While setting up the risk appetite, the following needs to be considered:-

- Financial strength of the company
- Regulatory requirement
- Risk Taking Capacity of the senior management
- Proposed business plans

Some components of the risk appetite can be quantified while others are more subjective and qualitative e.g. reputational risk.

(ii) Roles of Risk Management Committee

The purpose of the committee is to assist the board in its oversight of various risks. The committee:

- Approves and reviews compliance with risk policies, monitors breaches / triggers of risk tolerance limits and directs action.
- Reviews and analyses risk exposure related to specific issues and provides

oversight of risk across organization.

- Reviews reports of significant issues prepared by internal risk oversight functional groups, including risk exposure related to specific issues, concentrations and limits excesses.
- Nurtures a healthy and independent risk management function in the company Inculcates risk culture within the organization.
- Approves the Enterprise wide Risk Management (ERM) framework.

Composition and Term of Referance of the Risk Management Committee (RMC)

The RMC is the body responsible for the management of Risks in the Organization and it manages the same through oversight of the risk management function of the Company, and through approval of the various policies and processes of the Company.

The Committee reports to Board of Directors. DCL has constituted the executive level Risk Management Committee having executives representing various departments of the company. The TOR including constitution of RMC, Term of Reference, Reporting with frequency is attached with the policy.

(iii) Role of Audit Committee

As per RBI guidelines and as per the provisions of Companies Act, 2013, DCL has constitute an audit committee.

Audit committee shall evaluate the internal financial controls and risk management systems on quarterly basis. The risk management responsibility for the Audit committee will mainly be towards operational risk, as follows:

- Identifying and presenting operational risks in the course of regular internal audits with recommendations for corrective actions.
- Focusing the internal audit work for significant risks and auditing the risk management processes across the organization.

(iv) Senior Management

Senior Management will be responsible for the following: -

- Identifying and prioritizing the risks
- Prepare policies, systems, process & guidelines to reduce the risks.

(v) Middle Management

Middle Management will monitor the risks and adherence to them by branches

(vi) Branch Management

Branch management will do following things:-

- Implementation of risk management process through field staff
- Monitoring of adherence to the procedures

(vii) Field Staff

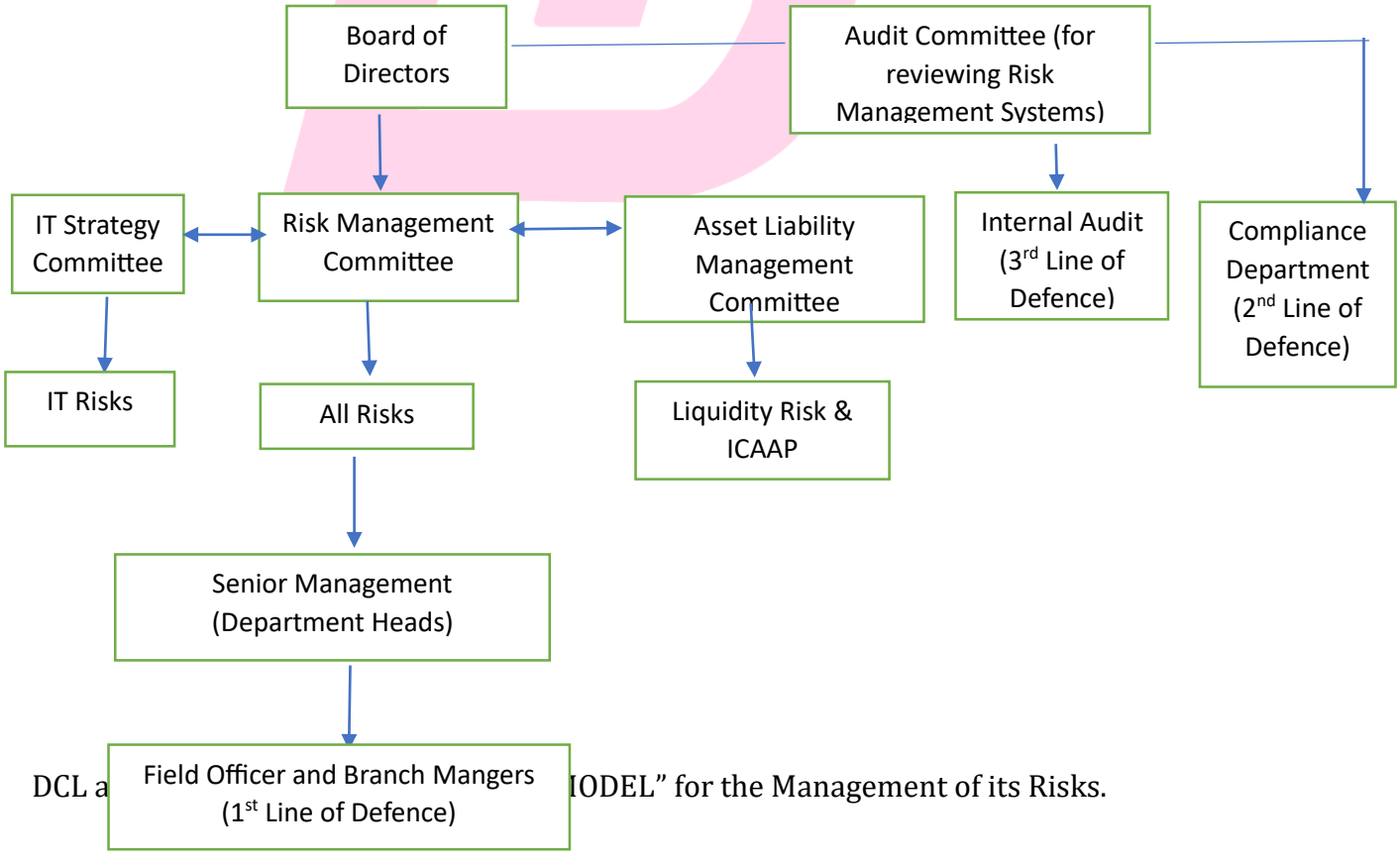
The field staff implements the procedures and offers feedback on the required changes

(viii) Internal Audit Department

Internal Audit Department: -

- Verifies that policies and procedures related to risk management are implemented properly
- Identifies deviations and detects early warnings and frauds

Management Structure of Risk Management in DCL



DCL a IODEL" for the Management of its Risks.

- The 1st Line of Defense will always be the Business and Support Units that will own the risks and manage the same, as per laid down risk management guidelines.

- The 2nd Line of Defense will always be the Compliance Department and the Legal Department that would support the 1st Line of Defense by the drawing up of suitable risk management guidelines from time to time to be able to manage the risks of the Company.

- The 3rd Line of Defense will always be the Audit Functions – primarily the Internal Audit functions that are supported by the External Audits, and other audits like Regulatory Audits, etc. The 3rd Line of Defense focuses on providing the assurance that the risk management principles/policies and processes are achieving the objective of managing the risks of the organization at all times. Please refer Chart given as Annexure 1

As of now DCL does not require to appoint a full time Chief Risk Officer or Risk Head and the Risk Management is divided among the department heads for their respective fields and works. The second line of defiance as of now will be with Compliance Department which will undertake the functions of Risk Manager.

The Compliance Department will undertake following functions/work:-

- Identification of risk points in the organization and assessing or measuring their impact on the business.
- Formulation of Risk Management Policies.
- Devising strategies for controls and mitigation of risks.
- Reports to Top Management, Risk Management Committee and Board of Directors on risk matters.
- Vetting of product policies in risk angle.
- Vetting credit proposals in risk angle.
- Assisting Credit units to develop Credit Assessment Models.
- Conduct portfolio analysis to measure migration in risk.
- Risk vetting of operational guidelines.
- Part of credit approval process.

The person nominated from compliance department will be invited in the meetings of ALCO, Credit Committee and other related committees.

Roles of various department in risk management

1. Compliance Department (Headed by CCO)

1. Anti Money Laundering (AML)
2. Know Your Customer
3. Combating the Financing of Terrorism
4. Process and Product (from compliance point of view)
5. Compliance of all applicable norms

2. CISO and IT Department

1. IT Related Risk
2. BCP & DR
3. Outsourcing
4. Party Management

2. Credit Department (Head-Credit)

1. Portfoio Risk Management
2. Credit process and underwritting

3. Finance Department (Headed by CFO)

1. Liquidity Risk
2. Reputational Risk
3. Asset and Liability Management

4. MIS Department

1. Forecasting
2. Statical Analysis

5. Business Strategy (Headed by CBO)

1. Economic Research
2. Strategic Analysis
3. Delinquency Management
4. Business and Product related Risk

6. Human Resource Department (Headed by Head-Human Resource Management)

1. Conduct Risk

2. Manpower Related Risk

Risk Reporting

Risk Management will not be completed without a structured process for reporting of risk related information, to all its stakeholders.

Risk Reporting therefore has two significant categories – Reporting to External Stakeholders and Reporting to Internal Stakeholders.

1. Risk Reporting to External Stakeholders:

External Stakeholders are always regulatory and legislative bodies. As a Financial Institution, that too one classified as a "Systemically Important" (SI) one, we have many a report to submit on risk related information – mainly from the Credit Risk side, but on the whole, these reporting cover an all round perspective of risks of the Company.

The Compliance Department will not only interact with the Regulators, it will advise all internal stakeholders on the relevant and extant reporting to be followed, from time to time.

2. Risk Reporting to Internal Stakeholders

Internal stakeholders are primarily

1. Board of Directors
2. Committees of the Board
3. Top Management Team
4. Functional Management Teams
5. Operational Stakeholders in all locations and departments

Thus, Risk Reports to Internal stakeholders can be classified as

- Strategic Reports on Risks – i.e. Reports that help formulate or review strategies
- Tactical Reports on Risks – i.e. Reports that help review the need for course-corrections
- Functional Reports on Risks – i.e. Reports that help measure the risk-metrics in a structured and consistent manner across all functional units of the company, and those that become the basic source of any MIS reports on Risks of the Company.

3. Reporting to the Managing Director, WTD, RMC & the Board of Directors on Risks

Periodic Reporting to Managing Director, WTD, RMC & the Board of Directors on Risks

The CCO will submit a detailed summary on quarterly basis on the overall Risk Status of the Company, based on the ERM Framework to RMC showing the Risk Heat Map and movement in the risk along with risk matrix along with deviations and action proposed to be taken regarding the matter to Managing Director, WTD, RMC & the Board of Directors.

RMC will give its recommendation to Board of Directors on the action to be taken on Risks.

4. Frequency of reporting

The reporting related to Risk Management will be done as per following frequency:-

S. No.	Person	Frequency
1	Board of Directors	Quarterly
2	Senior Management	Quarterly
3	Operational Teams	Quarterly
4	Others	As and when required

Chapter

3

CHAPTER 3: RISK MANAGEMENT PROCESS

What is Risk?

Risk is an 'uncertainty of outcome that affects the objectives' that is a two-sided coin, on one side it has threat, and on the other it has opportunity.

Risk is inherent to any business and NBFC-microfinance institutions (NBFC-MFI) are no exception. What makes NBFC-MFI special is absence or near absence of traditional risk mitigation mechanisms like collaterals and guarantees. Management of **Credit Risk**, therefore, becomes extremely important for NBFC-MFI. The monitoring, analysis and management of credit risk under group or individual lending models is core to the effective functioning of an NBFC-MFI.

All NBFC-MFIs face **Operational Risks**. Failure of a particular process, staff and client frauds, MIS failure are some of the risks that are common and have a direct bearing on the day to day functioning of the NBFC-MFIs.

The NBFC-MFIs are relying on the commercial bank funding. Increasing integration of the microfinance sector with the mainstream financial sector, together with diversification into new geographies not only adds complexity to the credit and operational risks but also create additional risks in the microfinance risk landscape. These additional risks that need proactive management are interestrate, liquidity and foreign exchange fluctuation, which can be collectively categorised as **Financial Risks.**

In addition, there is always a risk of failure of the strategic choices made by the NBFC-MFIs. Mission drift, competition, product development and governance are the issues that have come to the fore in the NBFC-MFIs. Therefore, there is a need for additional emphasis on **Strategic Risks** within NBFC-MFIs. A proactive and systematic management of all these strategic risks are important for the growth and sustainability of an NBFC-MFI.

Risks are hardly isolated; they are mostly interrelated. One risk will have a bearing on many other risks. An important aspect of understanding risks is developing an understanding of the interrelationships between them. Sometimes, a significant event

triggers reassessment of risks across the entire NBFC-MFI (i.e.across functions and product lines) precisely because of the interrelationships between different risks and the multiple impacts that a single event can cause.

Risks interact with each other

The risks above can be of many types given the specification and implications of the microfinance industry. Thus in such a scenario the identification of risk and adopting an appropriate mitigation strategy can be a complex task. It needs skills, preparation and commitment.

The increased emphasis on risk management in NBFC-MFI reflects a fundamental shift among managers and regulators to better anticipate risks, rather than just react to them. The NBFC-MFI must meet a series of qualitative standards including, the existence of an independent risk control and audit function and effective use of risk reporting systems.

Proactive risk management is essential to the long-term sustainability of an NBFC-MFI. It lays out the general framework for identifying, assessing, mitigating and monitoring risk in the NBFC-MFI as a whole. A key management responsibility is to provide reasonable assurance that the NBFC-MFI's business is adequately controlled, and until it has embraced risk management at an institutional level, there is very little chance that the NBFC-MFI's product-level risk management strategies can succeed.

Effective risk management has several benefits:

- **Early warning system for potential problems:** Less time fixing problems means more time for commercial business and growth.

- **Efficient use of capital:** Risk management allows management to qualitatively

measure risk, fine- tune the capital adequacy ratio, and evaluate the impact of potential shocks to the financial systemor institution.

- **Successful new product development and roll-out:** Systematically addressing the risks inherentin new-product development and roll-out can result in enhanced corporate reputation, improved customer loyalty, easier cross-selling of services, and better knowledge for developing future business.

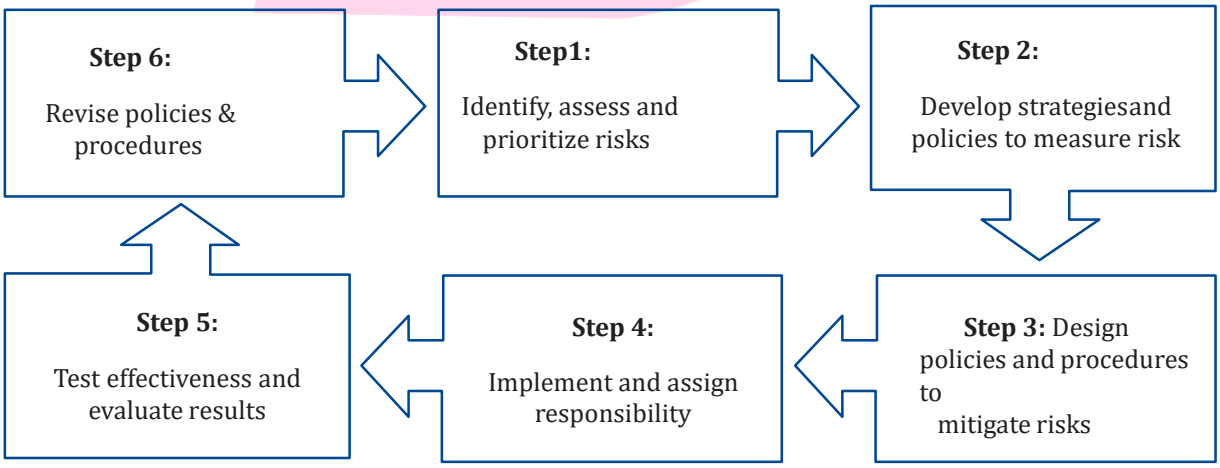
A Risk Management program must have following features:-

1. Lead from the top
2. Incorporate Risk Management into systems design
3. Keep it simple
4. Involve all levels of staff
5. Align Risk Management goals with individual goals
6. Address the most important risks first
7. Assign responsibilities and set monitoring schedule
8. Design informative management reporting to board
9. Develop effective mechanisms to evaluate internal controls
10. Manage risk continuously using a risk management feedback loop

Risk Management Process

Risk Management Process can be understood with following diagram

Risk Management Process Loop



Hence, the Risk Management Process involves following steps:-

Steps	Details
Step 1: Identify, assess and prioritize risk	Under this step the identification, assessment and prioritization of risk is being done by the Risk Owners i.e. the persons who are responsible as risk owners.
Step 2: Develop strategies and policies to measure risk	Under this step the Risk Management Committee develops the strategies and policies to measure the risk so that any of the following decision can be taken:- Risk Avoidance: DCL may choose to avoid risks which have high probability, are beyond its control and can have devastating effect on its functioning Risk Transfer: DCL may choose to transfer such risks which have low frequency but can be potentially devastating; examples of tools used for risk transfer are insurance and/or Hedging (wherever required) Risk Acceptance: If the probability of occurrence and the impact of a particular risk are minor and manageable relative to the cost of controlling it, DCL may choose to accept such a risk Risk Mitigation: If the likelihood of a risk is high and the impact of the risk is low to medium and the costs to manage it in house is also cost effective, DCL may try to mitigate such risks
Step 3: Design policies and procedures to mitigate risks	Designing of the policies and procedures regarding the risk mitigation.
Step 4: Implement and assign responsibility	During this step the mitigation plan is implemented and accordingly responsibilities are assigned
Step 5: Test effectiveness	Internal Audit or other responsibility centers test the effectiveness of the risk management process adopted by the

	company
Step 6: Revise Policy and Procedure	The policy and process related to Risk Management is reviewed and necessary actions for the improvement are taken

Implementing Strategic Risk Management System

Establish Objectives

The first step towards Strategic Risk Management Process is to establish the objective of the exercise. The objectives are to identify and mitigate the risks involved in the business and operations and thereafter establish the measures to mitigate those risks.

Identifying Risks

Risk analysis involves the identification of the risk components by answering the following questions:

- What is the risk event?
- What drives it? and
- How it can be monitored?

NBFC-MFI need to identify risk drivers, since it is the drivers that must be addressed. One symptom (high default rate), can represent one of several risk events (concentration of loan portfolio in one sector, clients do not or will not pay etc.), each of which may have a different set of risk drivers (drop in commodity price/increased cost of raw materials, inadequate monitoring procedures, poor client selection etc.). Each driver calls for a different mitigation strategy. Strengthening the NBFC-MFI's recovery procedures will not reduce the risk of a drop in prices in an industry that the MFI has invested heavily in.

Measuring and Prioritizing the Risk

The importance of risk events varies according to the probability of frequency and impact of occurrence. These risk assessments should determine the priority with which an NBFC-MFI allocates its resources to managing these risks. Whether the degree to which a risk is currently occurring within the organisation is considered a problem depends on the risk assessement and the related threshold.

NBFC-MFIs need to answer the questions: Can an institution accept certain levels of risk? If so, what are those levels and how can they be measured? The symptom that a risk is occurring (high default rate) in turn becomes a possible indicator (PAR 30) used to measure and monitor the level of risk. When a risk is being managed, it is likely that the symptoms will subside. In this manner, the symptom becomes an indicator that risk exposure is reduced. While this is reassuring, it does not answer the question, have we managed this risk sufficiently?

The use of indicators is extremely helpful in answering this question. Without data, MFIs cannot manage risk and cannot devise appropriate controls. Risks can be measured quantitatively and/or qualitatively, and both types of measurements are needed in order to provide balance. The indicators must be relevant to what is being measured. The measurements selected should be valid, objective and verifiable.

Criteria for Selecting Indicators

- Why are you measuring?
- What will you measure?
- How will you measure?
- Who will measure?
- Where will this be measured?
- When will this be measured?

Once the appropriate measure(s) have been decided, the NBFC-MFI must set the threshold for its risk tolerance, remembering controls have a cost as well as benefit. An NBFC-MFI may accept risk exposures up to a specified level, but above that threshold level, the NBFC-MFI must take further corrective action.

If the risk trend is not decreasing and is still operating outside of the desired thresholds, the identified risk drivers must be re-examined. If the real cause of the risk event has not been properly identified, then the tactics are unlikely to be effective since they are addressing the wrong driver.

This is very important step as based on measuring the risk, the process for prioritizing the same will be completed where priority for the risk mitigation will be given to those risks which has larger impact as per the measurement study.

Taking Action

Keeping in view of measurement of risk any of the following action can be decided by the management: -

1. Establishing the risk mitigation measures and implement them
2. Risk Transfer
3. Risk Avoidance
4. Accepting Residual Risk

Monitoring and reassessing

The risk management process including mitigation steps must be monitored and reassessed for taking corrective actions wherever required. The frequency for monitoring and reassessing will be once in a 3 months.

Risk inventory will be maintained in the format given as **Annexure 2**.

Chapter

4

CHAPTER 4: KEY RISKS

Risks and uncertainties form an integral part of DCL's business which by nature entails taking risks. Each transaction that DCL undertakes changes its risk profile. Following are the key risks identified by DCL:-

Credit Risk	Risk of default by Borrower
Operational Risk	Risks related to Process, People and Systems
Market Risk	Liquidity Risk and Risk related to Interest Rate
Strategic Risk	Emerging Risk and External Risk
Other Risks	Reputational Risk, Compliance Risk, Legal Risk, Currency Risk, Collateral position management and contingent liabilities related risk, conduct Risk, Human Capital Risk, outsourcing Risk, Settlement Risk, model Riak, IT Risk and Fraud Risk

Credit Risk: Credit Risk is the risk of loss due to the failure of the counter party to meet its credit obligations in accordance with the agree contract terms. It is the result of either inability or unwillingness of a borrower or counter-party to meet commitments in relation to lending or any other financial transactions.

There is always scope for the borrower to default from the commitments for one or the other reason resulting in crystallization of credit risk to DCL. These losses could take the form of outright default or alternatively, losses from changes in portfolio value arising from actual or perceived deterioration in credit quality that is short of default. The objective of credit risk management is to minimize the risk and maximize DCL risk adjusted rate of return by assuming and maintaining credit exposure within the acceptable parameters.

Operational Risk: Operational Risk is inherent in all product, activities, processes and systems of DCL. It is a risk of loss arising from inadequate or failed internal processes, people and systems or from external events. Risk education for familiarizing the complex operations at all levels of staff can reduce operational risk. Operational risk events are associated with weak links in the internal control procedures. Operational risk involves

breakdown in internal controls and corporate governance leading to error, fraud, performance failure, compromise on the interest resulting in financial loss.

Putting in place proper corporate governance practices by itself would serve as an effective risk management tool. DCL shall strive to promote a shared understanding of operational risk within the organization, especially since operational risk is often intertwined with market or credit risk and it is difficult to isolate.

Market Risk: Market Risk may be defined as the possibility of loss to DCL caused by the changes in the market variables. It is the risk that the value of on-/off-balance sheet positions will be adversely affected by movements in equity and interest rate markets, currency exchange rates and commodity prices. Market risk is the risk to DCL earnings and capital due to changes in the market level of interest rates or prices of securities, foreign exchange and equities, as well as the volatilities, of those prices. Market Risk consists of:

a) Liquidity Risk
b) Interest Rate Risk

Maintaining an optimal balance sheet structure and cash flow patterns shall be the keystone of the market risk management strategy.

A detailed description about managing market risks is available in the ALM policy.

Competition Risk: Competition Risk is the chance that competitive forces will prevent you from achieving a goal. It is often associated with the risk of declining business revenue or margins due to the actions of a competitor.

Liquidity risk: Liquidity risk arises where the Company is unable to meet its obligations as and when they arise. Liquidity risk will be measured at a structural level and a dynamic short term level. DCL may need to address liquidity risk and report to RBI on a periodic basis.

Interest rate risk: Interest rate risk management and reporting helps identify potential risks to earnings and capital resulting from adverse fluctuations in market interest rates.

Strategic Risk: Risks that derive from the decisions that the Management takes about the products or services that the organization provides. It include risks associated with developing and marketing those products or services, economic risks affecting service sales and costs, and risks arising from changes in the technological environment which impact on revenue.

It's a possible source of loss that might arise from the pursuit of an unsuccessful business plan. For example, strategic risk might arise from making poor business decisions, from the substandard execution of decisions, from inadequate resource allocation, or from a failure to respond well to changes in the business environment.

Strategic Risk needs to be assessed both in qualitative & quantitative terms. Assessment of an incidence or a potential risk aims at quantifying the risk in financial terms to the extent possible. Risk control shall be laid down by capturing various strategic risk assessment process/measures of success to help assessment it effective implementation and maintenance.

Reputational Risk: DCL is also exposed to reputation risk arising from failures in governance, business strategy and process, regulatory-compliance and legal risk. These risks are generally covered under Operational risks. Reputational risk is the risk of potential damage to the Company due to deterioration of its reputation. 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 procedures. Proactive measures to minimize the risk of losing reputation could be a sound risk management framework, good corporate governance, high level ethics and integrity, rigorous anti money laundering procedures, good business practices and reporting of all breaches which lead to reputational risk to the attention of senior management and the board.

Compliance Risk: Compliance risk is the risk arising from non-adherence to prescribed law in force, regulations, policies, procedures and guidelines which may give rise to regulatory actions, litigations, deficiency in product or services depending on the level of non- adherence. The corporate governance function is primarily designed to avoid incurrence of compliance regulatory-legal risk.

Legal Risk: The possibility of incurring losses or negative contingencies as a result of flaws in contracts or transactions that may affect the institution's legal position and/or ability to function; legal risks are a direct result of human error, fraud, negligence or carelessness in the design, formalization, application or implementation of contracts or transactions.

Legal risk is also caused by non-compliance with current laws or regulations.

Legal risk can primarily be caused by:

- A fraudulent transaction
- A claim including a defense to a claim or a counterclaim being made or some other event occurring which results in a liability for the company or other loss

- Failing to take appropriate measures to protect the company's interests including the assets owned by the company; or

Change in law which results in any of the transactions becoming illegal or bad in law or results on any of the above.

Currency Risk

Currency risk, or exchange rate risk, is the potential for financial loss due to changes in the value of one currency relative to another. The company is having External Commercial Borrowings (ECB) where servicing of the interest and principal is being done in foreign currency.

Collateral position management and contingent liabilities related risk

Collateral position management and contingent liabilities are both critical aspects of risk management, especially for financial institutions. Collateral management involves actively overseeing pledged assets to ensure they are sufficient to cover obligations and potential margin calls. Contingent liabilities, on the other hand, represent potential future obligations whose existence is uncertain and depends on future events. Effective management of both is essential to mitigate financial and operational risks.

Conduct Risk

Conduct risk refers to the potential for a company's actions or behaviors to cause harm to its customers, stakeholders, or the broader market. It encompasses ethical, moral, and legal standards, and is particularly relevant for NBFC-MFIs. Effective conduct risk management is crucial for mitigating the risk of regulatory actions and reputational damage.

Human Capital Risk

Human capital risk refers to the potential for loss or failure associated with an organization's human resources, impacting its ability to achieve operational, business resiliency, and continuity goals. It encompasses a range of issues stemming from employee behaviours, events, and the overall management of the workforce. These risks can lead to financial losses, reputational damage, and hinder strategic objectives.

Being an NBFC-MFI the Human Capital of DCL is very important to provide its services hence risk associated with Human Capital is identified and mitigation plans are made.

Outsourcing Risk

The company has outsourced its main technology i.e. LOS and LMS. The outsourcing risk is associated with material outsourcing. The Risk also associated with other material outsourcing which may be done by the company from time to time.

These risks include loss of control, communication barriers, security vulnerabilities, and potential quality issues.

Settlement Risk

Settlement Risk for an NBFC-MFI refers to the risk of loss arising when a counterparty does not fulfill its payment or delivery obligation after the NBFC-MFI has already met its end of the transaction. This may result in the NBFC-MFI not receiving the expected cash flows or assets within the agreed settlement timeline, adversely impacting liquidity and credit exposure.

The above risk is covered under Credit Risk and Liquidity Risk.

Model Risk:

Model Risk refers to the potential for adverse consequences arising from decisions based on incorrect or misused models. This includes errors in model design, data inputs, assumptions, implementation, or the use of the model beyond its intended scope. For an NBFC-MFI, model risk can significantly affect credit decisions, risk assessment, provisioning, and financial forecasting.

Information Technology Risk (IT Risk)

IT Risk, or Information Technology Risk, refers to the potential for loss or disruption resulting from inadequate, failed, or compromised IT systems, infrastructure, processes, or services. For an NBFC-MFI, IT Risk can significantly affect service delivery, data integrity, customer trust, regulatory compliance, and business continuity.

Fraud Risk

Fraud Risk refers to the possibility of financial or reputational loss resulting from intentional acts of deception, misrepresentation, or concealment by internal or external parties. For an NBFC-MFI, fraud may occur at any stage of the credit or operational cycle and can involve employees, customers, intermediaries, agents, or third-party service providers.

Physical Risk

Physical Risk refers to the potential for financial loss, operational disruption, or reputational damage due to the direct impact of environmental, climate-related, or external physical events. These risks arise from Robbery, fire, natural disasters, extreme weather, infrastructure failures that can affect the physical assets, staff, branches, and customer operations of an NBFC-MFI.

Socio Political Risk

Socio-Political Risk refers to the potential for financial, operational, or reputational losses resulting from changes in the socio-political environment, including government policies, political instability, civil unrest, regulatory shifts, or public sentiment. For NBFC-MFIs, such risks are particularly relevant given their grassroots presence, reliance on community engagement, and sensitivity to local and regional political dynamics.

Chapter

5

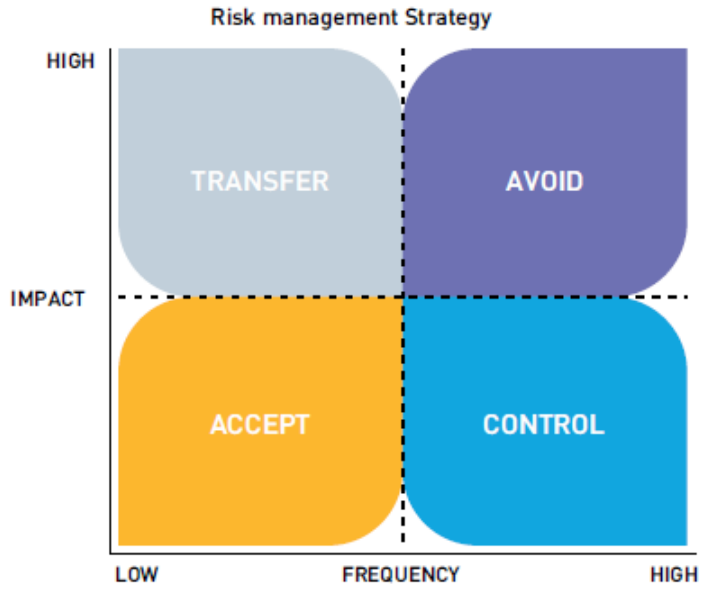
CHAPTER 5: RISK MANAGEMENT STRATEGY AND KEY RISK MANAGEMENT

Risk Management Strategy will be adopted based on the basis of likelihood and impact of the risk event.

Likelihood means what is the possibility of happening (frequency) of risk event and impact means what will be effect on the company if any risk event happens.

Risk Heat Map

Risk Heat Map shows the impact and likelihood of a risk event to happen and can be presented as under: -



The Risk Management Strategy has following 4 options:

Possible Strategy	When to be opted with example
Avoid	When likelihood and impact is very high e.g. Avoiding large ticket size loans, avoiding the problematic area, i.e. default areas or chronic disaster risk area
Transfer	When likelihood is low and impact is high, Transfer. e.g. Insurance against fire risk or Insurance against cash-in-transit.
Accept	When likelihood and impact is low, Accept. e.g. Loan losses in case, where all recovery measures are exhausted
Control/Mitigate	When likelihood is high and impact is low, Control. e.g. Most of the operational risks. Mitigation through Product design, Operational Processes, HR policy & Performance measures (PAR and ratio analysis)

Key Risk Management

1. Credit Risk Management:

Credit risk is the risk of failure of borrower to repay. This default by the borrower either be willful default or due to the reasons beyond the control of the borrower. To effectively manage the credit risk, which is a major risk in the microfinance, DCL continue to evolve the credit delivery procedures as the business grows. The following are some of the practices (only suggestive list) which may be adopted for mitigating this risk:-

(i) New Area selection:

- Before entering a new area for expanding the business, DCL shall do a due diligence using the pin code and check the credit bureau report to know the existing performance of other MFIs portfolio in that area. This will help DCL to avoid the known problem areas with a poor repayment track record.

- Apart from the secondary data research, DCL shall do primary research to know more about the area proposed for expansion as the quantitative data alone will not reveal the full picture, e.g. in many areas of a State, data may show that microfinance penetration is less, but the area may be having other problems like political influence.

- DCL shall make use of the Pin code level/district level reports shared by SRO or otherwise available to understand the trends in different operational areas.

(ii) Targeting of clients:

- Targeting women in rural areas.

- Preferring clients with their own houses.
- Avoiding clients who migrate during off-seasons.
- Focusing on clients who are involved in some income generation activities or intend to start the economic activity with the loan.
- Selecting clients with two livelihood income streams e.g. Agriculture + allied activities like dairy or poultry.
- Clients with proper KYC (Know Your Customer) documents viz Aadhaar card and Voter ID, duly verified with UIDAI through OTP. DCL may explore a systems which is QR code enabled, so that the Aadhaar card information can be auto-filled in the document without any error during the onboarding process.
- Clients Identity is verified through biometric authentication.

(iii) Focus on Basics of Group dynamics:

- After COVID-19 pandemic, many areas have still not reverted back to the center meetings, collections and field staff are making collections at the individual houses, which increases their time commitment in the field. Hence, DCL will focus on Basics of Group dynamics and will do its best efforts to re-start the center meetings.
- Conduct regular group meetings on specific dates and collections at the group meeting.
- Ensuring participation of all members in the group meetings.
- Proper updating of group records on a real-time basis during the meeting and recording the repayment collections in the group records from the members.
- Ensuring the peer pressure at the group level so that the social collateral i.e. joint and several liabilities can be enforced in case of defaults.
- Adequate Training (CGT-Continuous Group Training) of clients on group dynamics and loan products and processes, especially on pricing of loans and grievance redressal.

(iv) Sourcing of clients:

- Sourcing of clients within a radius of 15 to 20 kms from the servicing branch (to be extent possible).

- Clients should be selected only after the credit bureau check with any of the credit information companies.

- DCL may use Mobile apps through which the loan officers do the on-boarding process quickly and check the credit history with the credit bureau on a real time basis and this reduces the turnaround time and reduces the credit risk.

- DCL may use the Geo-tagging facility to tag their field staff to ensure that they enter the on-boarding data only from the field and the clients house coordinates are also mapped.

- Scorecard for Client Selection: DCL may develop a Scorecard for clients in association with Credit Bureaus with an objective of enabling the good customer selection and effective sourcing of clients for lending. The data are sourced from two sources viz. Data in application received from the client and the data from the credit bureaus. Customers are segmented into three categories viz. Existing customers with credit track record with DCL, New Customers with credit track record with other MFIs and New customers without credit track record. In variables (such as Age, Education, Occupation, Location (Rural or Urban), State, House (Own or Lease), Dependents in the family, Income, Expenses, FOIR ID cards (Aadhaar and Voter ID), How long as a customer?, Delinquency for various time periods (Last 30, 60, 90 days, 18 months & 24 months) in the past, Performance of Income generation loan Vs total loan outstanding of the borrower, Tenure, and term (Short term or Long term) of loans availed may be considered for arriving at the scores for clients and the variables combination varies for each of the 3 segments. Minimum credit score may be fixed For example, If the client is new without any credit history, they should have 730 credit score to get a loan, whereas for existing clients with DCL, a slightly lower credit score of 700 may be needed for the client to get loan. When the client score is high, they can be considered for additional loan amounts also. This will help DCL to source the good clients more effectively.

(v) Product design:

Products shall be designed in such a way so that the first loan borrower starts with a small size loan and the loan size will increase with every loan cycle.

(vi) Lending Process:

- DCL is having a written Credit operation manual explaining the step-by-step lending process and the same will be modified from time to time as and when required.

- DCL gives training to the field staff on credit operational processes so that the staff will do the due diligence properly and select the right borrowers.

(vii) Loan appraisal:

- DCL will ensure that the total monthly repayment obligations should not exceed 50% of the monthly household income. DCL shall capture the household income through the proxy indicators and estimate the FOIR (Fixed Obligations to Income Ratio) and ensure that it is not more than 50%.

- After doing a detailed working and study DCL may prescribe a range of FOIR to clients from different areas depending upon the risk expected. For example, clients from normal areas – Up to – 50% FOIR, and for clients from Risk prone areas (Flood prone or Drought prone areas), the FOIR may be kept at lower level – may be 40%.

(viii) Loan approval:

- DCL has centralized the loan approval process.

- DCL will explore to put filters to keep the portfolio growth within limits in various parameters and decisions on the clients already having loans with other financial institutions will be assessed accordingly.

(ix) Portfolio Diversification:

To avoid concentration of portfolio in certain geographies, DCL may set the ceiling for the geographical exposures at the state, District and branch level. The limits per branch, district and state are as follows-

Geographical location	**Limit**
State level	Upto 28%
District level	Upto 4 %
Branch level	Upto 2%

However, these limits can be reviewed by the management i.e. Executive Committee internally whenever needed as per the changed market dynamics and after assessing the situation and keeping in view of risk tolerance of the company the same can be modified. A report of the decision so taken will be submitted by the management i.e. Executive Committee to Risk Management Committee for its review and assessing change in risk.

(x) Loan documentation:

- During the loan documentation process, borrowers will be briefed about the loan sanction terms and conditions especially loan amount, interest rate, processing fees, insurance amount and repayment term & EMI.

- Borrowers signature will be obtained in the loan sanction letter for having accepted and understood the terms of the sanction.

(xi) Loan disbursement:

Loan disbursement will only be done after completion of the process and after doing the penny drop transaction in the bank account of the borrower to ensure the correctness of the bank account of the borrower through penny drop process.

DCL will explore the possibility of doing tele-call check before the disbursement to ensure that the right borrower gets the loan.

(xii) Portfolio analysis:

DCL shall analyse the performance of the portfolio according to ticket size, tenure, purpose, branch, sector, scheme-wise, state and so on and if any outlier in the trend is noticed, the case may be analyzed further and necessary actions are taken.

(xiii) Differential pricing:

DCL may offer risk-based pricing to retain the existing clients. For example, when compared with the new clients, the existing clients may get the loan at a cheaper rate for the repeat loans as the risk premium attached to the interest rate will be lower.

(xiv) Insurance:

- DCL takes the life insurance cover for the loan amount & for the loan term covering both the borrower and spouse.

- DCL through its Credit Hub or through its MIS Department or call center may also call nominees and brief them about the loan to the borrower.

(xv) Loan repayment:

- Close monitoring of loan accounts by the branch team and the immediate supervisors of the branch at frequent intervals must be done.

- Follow up on stressed assets (e.g. For SMA -2 accounts i.e. Overdues more than 60 days and up to 90 days) and NPA a/cs by a Head Office team.

(xvi) Natural Disasters:

The occurrence of natural disasters will also induce the credit default risk by the borrowers e.g. Loss of livelihoods due to the cyclone or floods. Loss of crops due to the drought. Loss of properties due to the earthquake hence while deciding the areas the natural calamity must be kept in mind.

(xvii) Client Protection principles & Code of Conduct:

- DCL shall follow the client protection principles and code of conduct to promote responsible lending so that the borrowers are not overindebted.

- DCL has put in place a proper grievance redressal mechanism and the contact details of the Grievance Redressal officers (Nodal Officer) is being made available to the clients and as well as have been displayed in the branches.

- DCL is already offering Toll-free numbers facility to the clients so that they can know their loan details (Loan amount, EMI paid, loan outstanding) in vernacular language and as well as voice their complaints to the Company.

(xviii) Internal Audit:

- DCL has ensured the Internal audit team's independence by making the Head-Internal Audit not to report to Sales, but to the Audit Committee directly.

- Internal audit teams will take up periodical visits to the branch based on risks (Branches are rated using a Risk rating framework periodically i.e. Low risks branch visited once in a quarter and Moderate risk branches visited bi-monthly and High risk branches visited monthly) and they verify whether all

the lending process steps have been followed by the branch or any deviations have been made.

- Apart from regular audits, Surprise snap audits shall be conducted by the Internal Audit team to keep a close vigil.

2. Operational Risk Management:

Operational risk is the risk of losses associated with the failure of the internal processes & systems or external events, or human failure or IT failure or frauds. The following are some of the practices (only suggestive list) which may be adopted for mitigating this risk:-

(i) Sourcing of clients:

- Clients with proper KYC documents (Aadhaar card and Voter ID card) are selected and verified with UIDAI through OTP.
- Digital verification of KYC documents eliminates the scope for frauds.
- Client's mobile number verification through OTP.

(ii) Product Design:

DCL shall focus on the product design to avoid the borrowers using the loan for some other purpose or borrowers seeking the additional loan from other sources as the loan product they availed has not served their specific needs. Both the situation will lead to delinquencies.

(iii) Loan Appraisal:

- DCL has a separate team i.e. Credit team to do the appraisal. Segregation of duties of sourcing and appraisal by different teams has been followed. Sourcing -Business team & Appraisal by Credit team ensures the objective appraisal and prevention of the selecting the ghost borrowers.
- House verification is done by the sales team and verified by credit team through geo tagging. Head office team may check the house site verification digitally through a video call but also engages with a Personal Discussion with the prospective borrower during the video call). This will also prevent ghost loans.

Loan appraisal is being done strictly as per the prescribed internal process.

(iv) Loan documentation:

Digital signing of loan documents may prevents ghost loan borrowers and also avoids paper use thus contributing to the SDG 13 (Sustainable Development Goal) of climate action. DCL will encourage the digital process of loan.

(v) Loan disbursement:

- Loan disbursements must be paid direct to the bank account of the borrower after doing penny drop.
- Verification of borrowers through tele-call before disbursement.
- Sending of the SMS to the mobile of the borrowers immediately after the disbursement.
- Post disbursement, tele-call team may make calls to the borrowers and checks the receipt of the loan amount by the borrower.

(vi) Loan repayment:

- Loan repayment collections preferred to be done in the group meeting and not in individual borrower's houses.
- DCL has entered into tie up with collection points of Banks and Payment bank's customer service points to deposit the cash collected by the loan officers at the nearest point instead of bringing it to the branch located in a far-off place to reduce the cash transit risk.
- Customer are encouraged to given loans through digital mode.
- Partial payment of the EMIs by borrowers must be checked carefully/stopped to avoid the fraud by field staff.
- Cashless repayment collections reduce the stress levels of staff drastically as they need not carry the cash from the centers to their branches and the time saved by the field officers can be optimally used by them for other tasks, resulting in increase of productivity.
- DCL may start sending SMS to the borrowers once they receive the repayment collections from the borrowers.

(vii) Monitoring:

- Regular monitoring by operational team at various level i.e. Branch level, Area level, Regional level and Territory level through weekly / monthly reviews must be done.

- Analysis of dash board reports (Indicators like Portfolio at Risk, SMA (Special Mention Accounts) and NPA movements, Provisioning, Write offs) closely and taking immediate action by Head office.

- DCL reconciles the Demand, Collection, Overdue and the amount collected Vs amount deposited in the bank on a daily basis and the dash board reports on unreconciled items is being shared with the field team immediately for their close follow up on the very next day.

- Comparing the Performance of portfolio of the region with the Industry portfolio and with the data of the last year same period to identify any patterns that requires proactive actions by the management.

- When supervisors go to field visits, they must go at random and without accompanied by the field officers

- While monitoring the progress or reviewing the performance targets achievement, the supervisors shall not force the field staff to achieve the business targets violating the processes or deviating from the ethics.

(viii) Post disbursement follow-up:

- DCL may conduct the loan utilization check by visiting the borrower's place.

- DCL may obtain the loan balance confirmation from the borrower every year or every 6 months.

- Even for regularly repaid loan accounts, random checks have to be done to check the hidden delinquency i.e. groups paying the EMIs instead of the borrower, as this may lead to a potential default in the near future.

(ix) Internal Audit:

- Internal audit team enters the branch at the opening time of the branch first and checks the cash at the branch and tallies with the cash book.

- Internal audit team verifies whether all the process steps including the maker/checker concepts followed by the branch.

- Internal audit team also verifies the borrowers in the field.

(x) Internal Control:

Prudent internal control measures have been put in place by the DCL viz.

- Maker – Checker model for approvals at every level.
- Dual control of keys of the safe at the branch
- Joint signatures for operating bank accounts
- Physical check-up of assets
- Data access on a need-to-know basis with proper log-in and passwords.
- Taking periodic trial balances and reconciliations.

(xi) Insurance:

DCL has taken the adequate insurance cover for covering cash-in-transit risk covering the cash snatching risks.

(xii) Information Technology:

- Periodical Data back-up taken and stored in a disaster free zone.

- Disaster recovery plan shall be in place to restart the operations immediately after the occurrence of any disaster event.

- IT audit will be taken up by DCL through a third-party agency on annual basis to check that effective control systems are in place.

- Detailed measures are covered in the relevant section.

(xiii) New Product/Process approval:

- All the new product and related process will be approved as per the policy for new product/process approval.

- DCL shall ensure that the Product/Process Approval Committee while checking the other aspects of the products before launch, shall have a thorough check of all possibilities for any risk from the new product/process.

- New Product/Process approval shall take care of the availability of IT controls and controls for ensuring the compliances to the statutory and regulatory requirements.

(xiv) Clients Satisfaction Survey:

DCL may conduct the Clients Satisfaction survey to know how far clients are satisfied with its products and services and accordingly should take further action in the matter.

(xv) Field officer rotation:

As the microfinance business involves close interactions with the clients, when a field officer leaves the company, that field officer also takes away the micro-level knowledge about the clients and it takes at least 3 to 6 months for a new staff coming to this position to close this knowledge gap. This transition period of 3 to 6 months is highly risky for the company and it opens up opportunities for operational risk. Hence, DCL may focus on retaining the field staff and as well as practice the staff rotation at the field officer level.

(xvi) Strong second level:

In Microfinance operations, people in all functional roles accumulate lot of specific experience related to their context and once they leave the company, that wisdom goes with them and creates problems in the transition period as the new person coming in that place takes a reasonable time to rebuild the lost connection between the company and the people. So, company can place the second level persons at every management level – Assistant Branch manager at the Branch, Assistant Area Manager or Assistant Regional Manager at area/regional level so that the transition periods can be effectively handled by the company without any risk to the underlying portfolios.

(xvii) Training to Clients:

- DCL gives training to clients on various products and especially on the interest rates and other fees that they have to pay. As per the RBI guidelines, the factsheet containing all details regarding the loan should be given to clients to make them understand that they have taken an informed decision.

- DCL also give training on financial literacy for enhancing the financial literacy among borrowers.

(xviii) Group Level Records:

- Field Officer shall insist that the group leaders record the loan repayment collections made in the group meeting in the group records during the meeting itself.

- Loan cards issued to the borrowers shall be properly filled in as and when the borrower repays the monthly instalments. This will be checked by the Internal Auditors also.

3. Liquidity Risk Management:

Liquidity risk is the risk of a situation wherein an NBFC (company) is not having sufficient cash and liquid funds to pay for the loan repayment obligations and its operational expenses. If Bankers perceive that any company is not liquid or if the bankers see a large scale defaults in an area, they stop further funding to that company, which results in immediate downgrade of the rating of that company, which aggravates the situation and other risks also emerges (due to the shortage of funding, when disbursal is stopped by the company, the clients stop the regular repayment forcing the credit risk default).

As per the requirement prescribed by RBI the company has formed the ALCO (Asset-Liabilities Management Committee), which is responsible for ensuring adherence to the risk tolerance/limits set by the Board and as well as implementing the liquidity risk management strategy. ALCO decides on the desired maturity profile and mix of incremental assets and liabilities, sale of assets as a source of funding, the structure, responsibilities, and controls for managing liquidity risk, and overseeing the liquidity positions of entire company.

The best practices for managing the liquidity risks are as follows:

(i) Diversification:

The Company will plan and manage its fund requirements in a manner that it does not depend on a single lender and accordingly shall diversify the borrowing sources – Public sector banks, Private sector banks, NBFCs and other lenders. The company will ensure a perfect mix of various borrowing methods such as CC, Term Loan, DLOD, CP, ECB, NCDs etc.

(ii) Minimum Liquidity:

- The company shall have cash and liquid funds equal to at least 3 months of loan repayment obligations and operational expenses. Of course, it will have a negative carry cost which should also be managed accordingly.

- To reduce the negative carry cost, an amount equal to the amount which carries negative carry cost, may be raised at a comparatively lower rate through the instruments like CP (Commercial Paper).

(iii) Asset-Liability Matching:

- The Company shall borrow for long term and lend for short term so that company will not face the asset-liabilities mis-match.

- Statement of Structural Liquidity will be prepared by the company by placing all cash inflows and outflows in the maturity ladder according to the expected timeline of cash flows so as to find out the liquidity gaps in different time buckets. The company shall ensure that there is no short term (30 days) negative mismatches above the prescribed limits.

(iv) Diversified Instruments:

The company shall diversify the financial instruments through which it raises equity or debt viz Equity, Subordinated debt, Term loans, Working capital loans, ECB (External Commercial Borrowing), NCD (Non-Convertible Debentures), Impact Bonds, Commercial Paper, Compulsorily Convertible Preference Shares and so on.

(v) Raising fresh Equity Capital:

- Even though banks are comfortable with giving loans up to 5 to 6 times of the own funds, the company shall start planning the equity raise once it reaches the borrowing equal to 4 or 4.5 times of their own funds.

- During the liquidity crisis, when promoters bring in their own funds, it gives the confidence to the lenders and investors and they will also reciprocate by extending their funding to the company and this will enable the company to navigate the liquidity crisis (if any) soon.

(vi) Covenants of Financing Institutions:

- The company shall closely monitor the funding covenants (Common funding covenants include Portfolio at Risk, Write-off, Capital Adequacy Ratio (CAR), Profitability and non-funding covenants like change in ownership, changes in senior management, mergers & acquisitions, change of business) of financing institutions carefully, as the breach of funding covenants will be treated as

"Event of Default" and necessary actions will be triggered by the lenders, including stoppage of lending.

- To avoid the breach of covenants, the company may plan to have more provisions as a buffer during the good years, which will help it to absorb the unexpected shocks during the bad year.

(vii) Liquidity Contingency Plan (LCP):

- Liquidity Contingency Plan shall identify the early warning signals to the liquidity risk, fix roles & responsibility to a specific person, keep open the channels of communication with the lenders and investors.

- LCP will also identify the potential contingency funding sources and the amount/estimated amount which can be availed from these sources, well-structured escalation/ prioritization procedures detailing when and how each of the actions shall be activated, and the lead time needed to avail the additional funds from each of the contingency sources.

(viii) Liquidity Coverage Ratio (LCR) and Stock and other Ratios :

- Liquidity Coverage Ratio of the company shall be calculated as given below.

$$\text{LCR} = \frac{\text{Stock of High-Quality Liquid Assets}}{\text{Total Net Cash Outflows for the next 30 days.}} \times 100$$

- LCR shall be kept at the level as may be decided by the ALCO from time to time.

The ALCO shall be discussing various other ratios related to liquidity risk including stock ratios and the same shall also be placed before Risk Management Committee for analyzing the same from risk management point of view.

(ix) Postponing the Capital expenses:

To manage the liquidity problems, the company may postpone the expansion plans thereby reducing the capital expenses and conserve the cash.

(x) Stress testing:

- The company shall conduct stress tests on a regular basis for different short-term and protracted NBFC-specific and market-based stress scenarios (individually and in combination) and for survival horizon.

- While designing liquidity stress scenarios, the nature of the Company's business, activities and vulnerabilities shall be taken into consideration so that the scenarios incorporate the major funding and market liquidity risks to which the company is exposed.

4. Governance Risk Management:

Governance risk is the risk of Board of the company failing to deliver its duty to provide the necessary oversight and strategic direction. The results of governance failure will lead to the collapse of the company.

Corporate governance of the company provides the structures and processes by which company is directed and controlled. Good corporate governance helps the company operate more efficiently, improve access to capital, mitigate risk, and safeguard against mismanagement. It makes company more accountable and transparent to investors and other stakeholders and offers them the tools to respond to emerging concerns.
The suggestive best practices for mitigating the governance risks are as given below:

- The company will keep its Board professional by having more no. of Independent Directors.
- Board shall ensure the independence of the audit process and put in place a clearly defined risk management system and monitor the risks closely & mitigate the risks.
- Independent Directors shall keep asking the right questions to the promoters and key managerial persons to avoid the transactions involving conflict of interest.
- Board shall promote the organizational culture by nurturing the values like integrity, transparency, honesty from the top to down the line.
- Board shall evolve a transparent process for decision making and fix accountability to specific roles in the management.
- Board members may take up field visits and keep open the feedback loops, especially the negative feedback loops so that they can detect the early warning signals and take corrective actions at the budding stage of the problems.
- Board shall keep sufficient internal checks and balances over the executive's decisions on related party transactions and generous compensation practices for senior management.

- Board shall ensure the balancing of financial and social objectives of company and staff is focused both on "Profit and Purpose-making a difference in the lives of clients and staff and serving all the stakeholders

- Board shall make proper disclosures and oversee that the statutory and regulatory compliances are complied with by the company on time.

- The company may take the Directors and Officers liability Insurance cover to protect its Directors and Top management members.

Incorporation of Liquidity Costs into Pricing and Performance Measurement

The Company shall implement a structured process to quantify and allocate liquidity costs across products, in alignment with sound risk management practices. This includes:

- Estimating the cost of maintaining adequate liquidity buffers, funding mismatches, and market liquidity risks.
- Incorporating liquidity costs into internal product pricing models, ensuring all pricing decisions reflect the true economic cost of funds.
- Including liquidity cost assessment as a critical input in:
    - Performance measurement of business units
    - Profitability analysis
    - New product approval processes

The Finance Department shall jointly define and periodically review the methodology used for calculating liquidity costs, with oversight from ALCO (Asset-Liability Committee).

Internal Rate of Return (IRR) and Net Interest Margin (NIM) Strategy

To ensure sustainable profitability and risk-adjusted returns, the Company shall develop and adopt a formal strategy for the management of IRR and NIM, which shall include:

- Periodic assessment and monitoring of IRR for all products, with clear benchmarks and thresholds.
- Identification of key risks to IRR and NIM, including interest rate volatility, funding mix changes, prepayment risks, and competitive pricing pressures.
- Use of scenario analysis and stress testing to evaluate the impact of adverse movements in interest rates and liquidity conditions on IRR and NIM.
- Establishing early warning indicators and limits to detect and respond to erosion in IRR and NIM targets.
- Incorporating IRR/NIM risk assessments into the product development, pricing and portfolio review processes.

ALCO shall be responsible for oversight of IRR and NIM strategies and shall report key deviations and risks to the Risk Management Committee on a quarterly basis.

5. Reputation Risk Management:

Reputation risk is the risk of loss due to negative perception of the public, authorities on account of unethical practices and lack of transparency in pricing by Company. The suggestive best practices to mitigate the reputation risks are as follows.

(i) Communication:

All terms and conditions of the loan shall be clearly communicated to the borrowers in vernacular language.

(ii) Transparency:

- As transparency in operations of company will build trust among the stakeholders, Company shall be transparent in loan delivery process and especially pricing of loans.
- Loan cards shall be issued which show the loan amount, repayment term, interest rate, processing fees and insurance details.
- Pricing information shall be furnished to the borrowers through a standardized fact sheet.
- Company shall prominently display the minimum, average and maximum interest charged by them on the microfinance loans at all its offices and on the website.

(iii) Fair Practice Code:

- The company shall display the Fair Practice Code at all its offices and also on the website.
- The company shall follow the client protection principles and shall ensure responsible lending.

(iv) Recovery of loans:

The company shall ensure that its staff or agents (if appointed) are not engaged in harsh recovery methods.

(v) Credit Plus activities:

The Company may start credit plus activities and may offer non-financial services to the clients to add value to them. For example, offering Entrepreneurship development training to the clients. This will create a positive image for company in the eyes of public and government authorities.

6. Cyber Security Risk Management:

Cyber security risk is the risk of a possible threat of potential disruption to the business or to a business reputation by a cyber-attack. Cybercrime attackers steal confidential data from the system and disrupt the business operations of the companies. The best practices in Cyber security risk mitigation are as given below.

- Board and committees shall invest quality time to discuss on the emerging cyber security risks and may bring in good quality talents for tackling cyber security risks.
- The company shall educate its staff not to click the links sent by the third parties through email or SMS.
- The company shall ensure that the systems are secured by anti-virus.
- For approving financial transactions, the company shall have 2 step authentications.
- Provision of middle ware so that the members cannot reach the backend and front end directly.
- VAPT (Vulnerability Assessment and Penetration Test) shall be done annually through a Third party.
- Emails from unknown sources shall not be opened.
- Creation of strong passwords, keeping the passwords confidential and changing the passwords often.
- Ensure that the web pages visited are secure. When the web page you are browsing start with https:// and have a lock-sign, it means that the web page you visit is secure and encrypted for security.

Other than above there shall be a detailed cyber security program which will be reviewed and updated from time to time.

7. Crisis Risk Management:

MFI industry is known for the crisis for example crisis related to demonetization and recent crisis related to COVID-19. Following are some suggestive crisis risk mitigation measures which may be adopted by the company: -

- Executive Committee shall put in place a Business Continuity Plan (BCP), which is a written plan that sets out the processes and systems that are needed to continue or restore the operations of the company in the event of a crisis or disruption.

- Executive Committee shall take up an initial assessment of the impact of the crisis and shall form a "Crisis Management Committee" to take immediate action.

- Executive Committee shall have meetings often – either weekly or bi-weekly and this will enable the Board to give oversight guidance on time.

- Executive Committee shall keep the lines of communication open and shall communicate to all the stakeholders – investors, regulator, government, banks, staff, clients and vendors.

- Executive Committee shall be transparent sharing both the good news as well as bad news with the stakeholders, that will build up the trust in company among the stakeholders.

- Executive Committee shall prioritize the management to keep a focus on nurturing good relationship during the crisis with all stakeholders. Good rapport with the stakeholders during the crisis, will enable the MFIs to get their support. Especially this will be crucial for fund raising during the critical time and tough times.

- Executive Committee shall delegate more powers down the line as during the crisis, some situations need faster responses and decisions have to be taken at the field level. Boards shall make the processes so flexible to suit the emerging situation.

- Executive Committee shall think big and wild to spot out the opportunities hidden in the crisis and shall focus on that.

- Executive Committee shall enlarge the feedback loop so as to get to know the changing aspirations of the clients and staff and Boards can ensure the revision of the products and processes and add new products & services to deepen their services to the clients.

- Executive Committee shall spread positivity and hope among the stakeholders and this will give confidence to the front-line staff to deliver the services even during the critical times of crisis period.

- Executive Committee shall ensure that the company have a continuous dialogue with the Govt and regulator during the crisis.

- Executive Committee shall give directions to the senior management for the schemes announced by the government and the regulator.

- Executive Committee shall ensure the liquidity of the company and shall take action to improve the liquidity position by availing special lines of credit to boost the liquidity to keep the funds flowing in the business.

- Executive Committee shall keep an eye on the expenses especially defer the capital expenses and not to cut the salaries of staff or benefits of staff to reduce the operational expenses, as this will affect the morale of the staff.

- Executive Committee shall ask the senior management to do a stress testing exercise with different scenarios to plan for the cash flow.

- Executive Committee shall ensure the safety and well-being of the staff and clients during the crisis.

8. **Other Risks and their management** (these are only suggestive risks and Risk Management Committee from time to time may during the course of its function may identify other relevant risk also along with the mitigation plan)

A. Currency Risk Management

Currency risk, or exchange rate risk, is the potential for financial loss due to changes in the value of one currency relative to another. The company is having External Commercial Borrowings (ECB) where servicing of the interest and principal is being done in foreign currency.

Currency Risk Management Strategies:

1. Natural Hedging

- Align foreign currency inflows with outflows (e.g., borrowing and repayments in the same currency).
- Match tenure and currency of assets and liabilities wherever possible.

3. Financial Hedging Instruments

- Use derivative contracts like:

- **Forward Contracts**: Lock in exchange rate for a future date.
- **Currency Swaps**: Exchange fixed interest payments in one currency for another.
- **Options**: Right (not obligation) to exchange currency at a fixed rate.

Note: Derivatives must comply with RBI's guidelines under FEMA and be used only for hedging and not speculation.

4. ECB Hedging Policy

- RBI mandates a **minimum hedge coverage** for ECBs:
  - 100% hedging for average maturity <5 years (as per current ECB guidelines).
  - NBFCs must comply with RBI circulars on hedging under ECB framework.

5. Internal Limits & Monitoring

- Set internal **Value at Risk (VaR)** or **Net Open Position (NOP)** limits.
- Regular monitoring and reporting to RMC of FX exposure and sensitivity analysis.

6. Periodic Stress Testing & Scenario Analysis

- Analyze impact of currency depreciation (e.g., INR/EUR at 10%, 15% drop) on cash flows, profitability, and leverage ratios.

B. Collateral position management and contingent liabilities related risk

Collateral position management and contingent liabilities are both critical aspects of risk management, especially for financial institutions. Collateral management involves actively overseeing pledged assets to ensure they are sufficient to cover obligations and potential margin calls. Contingent liabilities, on the other hand, represent potential future obligations whose existence is uncertain and depends on future events. Effective management of both is essential to mitigate financial and operational risks.

Collateral Position Management:

Purpose:

To ensure that a sufficient amount of high-quality collateral is available to cover borrowing needs and potential margin requirements.

Risk Mitigation:

Adequate collateral management helps prevent liquidity crises, minimizes potential losses from margin calls, and ensures the ability to meet obligations during stressed market conditions.

Key Activities:

- Monitoring the value and location of pledged assets.
- Distinguishing between encumbered and unencumbered collateral.
- Calculating collateral positions and evaluating margin requirements.
- Identifying and managing operational and liquidity challenges related to collateral.

1. Collateral Register

- Register to have following information:
    - Eligible asset classes (e.g., loan receivables, fixed deposits, property)
    - Haircuts/margins to be applied
    - Frequency of valuation
    - Custody, control, and substitution rules

2. Legal Due Diligence and Perfection of Security

- Ensure proper documentation and execution of loan/security agreements.
- Registration of charges with **CERSAI**, **ROC**, or relevant authority (as applicable).
- Verify title, ownership, and enforceability of collateral before recognition.

3. Collateral Monitoring

- Implement a **system fo quarterly monitoring** to track:
    - Current value of pledged assets
    - Margin requirements and utilization
    - Exposure-to-collateral ratio
    - Eligibility status

4. Periodic Revaluation of Collateral

- Perform periodic revaluation of collateral assets:
    - Receivables portfolio: Based on aging, NPA classification, or ECL ratings.
    - Physical assets: By empanelled valuers at defined intervals.

- Apply appropriate **haircuts** based on asset type, credit quality, and market volatility.

D. Contingent Liabilities:

Definition:

A potential obligation that may arise from past events, but its existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the entity's control.

Examples:

- **Guarantees:** A promise to pay another party's debt if they default.
- **Warranties:** Obligations to repair or replace defective products.
- **Litigation:** Pending lawsuits where the outcome is uncertain.
- **Government programs:** Commitments to provide financial assistance in specific situations.

Risk Mitigation Strategies:

1. Identification and Classification

- Maintaining a **Contingent Liability Register** capturing:
    - Nature of obligation
    - Counterparty
    - Amount involved
    - Probability of occurrence
    - Likely impact
    - Stage of resolution (e.g., legal case status)

2. Assessment and Materiality Review

- Periodic review by the **Risk Management Committee (RMC) and ALCO**
- Classify based on likelihood (remote, possible, probable) and severity.
- Perform scenario analysis to evaluate potential impact on capital and liquidity

3. Using in Stress Testing

- Consider in ICAAP and stress testing frameworks.

5. Disclosure and Governance

- Transparent disclosure of significant contingent liabilities in:
  - Financial statements (notes to accounts)
  - Board and audit committee reports
  - ICAAP documentation and investor reports

C. Conduct Risk

Conduct risk refers to the potential for a company's actions or behaviors to cause harm to its customers, stakeholders, or the broader market. It encompasses ethical, moral, and legal standards, and is particularly relevant for NBFC-MFIs. Effective conduct risk management is crucial for mitigating the risk of regulatory actions and reputational damage.

Key Aspects of Conduct Risk:

Customer Harm:

Conduct risk includes the potential for company to engage in practices that harm customers, such as unfair treatment, unsuitable product recommendations, or inadequate disclosures.

Stakeholder Impact:

It also covers actions that negatively affect other stakeholders, including employees, shareholders, and the wider market.

Risk Mitigation Strategies:

1. Code of Conduct and Ethical Standards

- Implementing of **Code of Conduct**, applicable to all employees, field staff, and agents.
- Clearly define acceptable behaviors, red lines, and disciplinary consequences.
- Include guidelines on customer communication, field behavior, group meeting protocols, and complaint handling.

2. Field Staff Training & Certification

- Mandatory **induction and periodic refresher training** on:
  - Customer rights and protection

  - RBI Fair Practices Code
  - Grievance redressal procedures
  - Gender sensitivity and inclusion
- Use real-life case studies and role-play exercises to reinforce ethical behavior.

3. Customer Education & Transparency

- Provide customers with:
  - Loan cards with interest, charges, and repayment schedule
  - Pre-disbursement counseling sessions (CGT and GRT)
  - Loan agreement in local language
- Obtain signed customer declarations post-counseling.

4. Grievance Redressal Mechanism

- Multi-tiered grievance resolution system:
  - Field-level resolution
  - Branch/area escalation
  - Centralized Grievance Officer
- Display helpline number and escalation matrix in branches and group meetings.
- Maintain grievance MIS and analyze trends for systemic improvements.

D. Human Capital Risk

Human capital risk refers to the potential for loss or failure associated with an organization's human resources, impacting its ability to achieve operational, business resiliency, and continuity goals. It encompasses a range of issues stemming from employee behaviours, events, and the overall management of the workforce. These risks can lead to financial losses, reputational damage, and hinder strategic objectives.

Being an NBFC-MFI the Human Capital of DCL is very important to provide its services hence risk associated with Human Capital is identified and mitigation plans are made.

Key aspects of human capital risk:

Operational Risks:

These include risks related to fraud, theft, workplace safety incidents, and non-compliance with procedures.

Business Resiliency and Continuity:

Human capital risks can impact an organization's ability to maintain operations during disruptions, such as pandemics or other crises.

Talent Management:

Risks related to talent acquisition, development, and retention are crucial, including talent scarcity, high employee turnover, and leadership gaps.

Employee Engagement and Performance:

Dissatisfaction, reduced productivity, and misconduct can all pose risks.

Compliance and Regulatory:

Organizations must also manage risks associated with compliance with labor laws and regulations.

Examples of human capital risks:

Employee Turnover:

High turnover can lead to loss of knowledge, skills, and productivity, as well as increased recruitment and training costs.

Leadership Gaps:

Lack of effective leadership can hinder decision-making, employee motivation, and overall performance.

Negligent Hiring:

Poor hiring practices can lead to unqualified or unethical employees, increasing the risk of misconduct and operational failures.

Workplace Safety Incidents:

Accidents and injuries in the workplace can result in significant costs, including medical expenses, lost productivity, and potential legal liabilities.

Compliance Violations:

Failure to comply with labor laws and regulations can result in fines, penalties, and reputational damage.

Data Breaches:

Employees can be a source of data breaches, either intentionally or unintentionally, leading to significant financial and reputational losses.

The company shall review the above risk and shall design and monitor the mitigation plans.

Risk Mitigation Strategies

1. Robust Talent Acquisition Strategy

- Streamline recruitment with clear role definitions and selection criteria.
- Build a recruitment pipeline in advance for field operations.
- Use background verification and behavioral assessments, especially for customer-facing roles.

2. Structured Onboarding and Induction Programs

- Develop standardized induction modules focusing on:
    - Organizational values and mission
    - Regulatory compliance and RBI fair practices
    - Customer service and conduct expectations

3. Training and Capacity Building

- Implement periodic training calendars for all levels of staff.
- Include topics such as:
    - Credit underwriting and collection ethics
    - Technology usage (LMS/MIS apps)
    - Financial literacy and gender sensitivity
- Track training effectiveness through assessments and field observations.

4. Retention and Incentive Mechanisms

- Design performance-linked incentive (PLI) schemes aligned with responsible practices.

- Offer non-monetary benefits such as recognition programs, learning opportunities, and career progression tracks.
- Periodically review compensation to remain competitive.

5. Succession Planning & Talent Mapping

- Identify key roles and build succession pipelines.
- Develop internal leadership through Management Trainee Programs and Fast Track Growth Paths.

6. Employee Engagement and Well-being

- Conduct employee satisfaction surveys, grievance redressal forums, and field feedback sessions.
- Promote work-life balance, field safety SOPs, and mental health awareness campaigns.
- Offer insurance and health benefits to mitigate personal risk.

7. Compliance & Ethics Monitoring

- Deploy a Code of Conduct and HR Manual covering ethics, disciplinary process, and conflict of interest.
- Implement whistleblower channels and periodic staff audits.

8. Digitization and Automation of HR Processes

- Using of HRMS platforms for:
    - Attendance and leave management
    - Goal setting and performance appraisal
    - Training tracking and compliance alerts

E. Outsourcing Risk

The company has outsourced its main technology i.e. LOS and LMS. The outsourcing risk is associated with material outsourcing. The Risk also associated with other material outsourcing which may be done by the company from time to time.

These risks include loss of control, communication barriers, security vulnerabilities, and potential quality issues.

Risk Mitigation Strategy

1. Governance and Policy Framework

- Outsourcing Policy: Establish a comprehensive board-approved outsourcing policy specifying due diligence, risk assessment, approval authority, and periodic review.
- Risk Categorization: Classify outsourcing arrangements as "material" or "non-material" and apply enhanced oversight on material contracts (e.g., core IT systems, KYC, loan management software).

2. Due Diligence and Vendor Selection

- Risk Assessment: Evaluate vendor's financial soundness, reputation, legal compliance, operational capability, data security standards, and business continuity preparedness.
- Background Check: Perform checks for regulatory compliance, litigation history, and cyber audit reports.
- Multiple Vendors: Avoid concentration by diversifying vendors for critical services (applicable in cases other thean IT outsourcing).

3. Contractual Safeguards

- SLAs and KPIs: Clearly define performance metrics, penalties, and remedial actions.
- Right to Audit: Include audit and inspection rights by the company or regulators.
- Sub-Contracting Clause: Prohibit sub-contracting without prior approval.
- Termination Clause: Ensure exit rights in case of non-performance, regulatory instructions, or vendor insolvency.
- Confidentiality & Data Security: Enforce non-disclosure, secure data handling, and storage clauses aligned with RBI and UIDAI norms.

4. Monitoring and Oversight

- Vendor Performance Reviews: Conduct regular monitoring against SLAs and KPIs.
- Reporting: Escalate non-compliance to the Risk Management Committee or Audit Committee.
- On-site Assessments: Periodic visits to vendor premises to check controls and compliance.

5. Business Continuity and Contingency Planning

- Exit Management Plan: Ensure smooth transition of service without disruption.

- Data Migration Plan: Ensure data portability in a secure format.
- Business Continuity Agreement: Ensure vendor has disaster recovery systems aligned with the company's BCP framework.

6. Regulatory Compliance

- RBI Guidelines Adherence: Comply with RBI Master Directions on Outsourcing (latest applicable circulars for NBFCs).
- Material Outsourcing Reporting: Report material outsourcing arrangements to the Board/RBI as required.
- Data Localization: Ensure compliance with data residency and UIDAI norms for AUA/KUA or CKYC services.

7. Internal Controls and Training

- Internal Audit Review: Include outsourcing arrangements in the scope of internal and IT audits.
- Training: Train staff on outsourced process monitoring and escalation procedures.

8. Cybersecurity and Data Privacy

- Data Sharing Protocols: Encrypt sensitive data transfers and ensure firewalls & access controls.
- Breach Response Plan: Set up a defined incident response framework in collaboration with the vendor.

9. Board and Senior Management Oversight

- Regular Reporting: Periodic updates to the Board and RMC on outsourcing risks and incidents.
- Material Risk Escalation: Any significant risk events must be escalated to the senior management immediately.

F. Settlement Risk

Settlement Risk for an NBFC-MFI refers to the risk of loss arising when a counterparty does not fulfill its payment or delivery obligation after the NBFC-MFI has already met its end of the transaction. This may result in the NBFC-MFI not receiving the expected cash flows or assets within the agreed settlement timeline, adversely impacting liquidity and credit exposure.

The above risk is covered under Credit Risk and Liquidity Risk.

G. Model Risk:

Model risk arises when financial or operational models used for decision-making (e.g. credit scoring, provisioning, pricing, stress testing, forecasting) produce inaccurate, misleading, or incomplete results due to flaws in design, implementation, data quality, or inappropriate use.

Risk Mitigation Strategy

1. Model Governance Framework

Model Inventory: Maintain an updated inventory of all models used across departments (credit, finance, risk, collections, analytics).
Ownership Structure:

- *Model Owner*: Responsible for development and performance.
- *Model Validator*: Independent review unit (can be internal or external).
- *Model User*: Business or operational units using model outputs.

2. Model Development Standards

- **Design Protocols:** Follow structured design principles including objective, assumptions, data sources, version control, and performance metrics.
- **Robust Testing:** Back-testing and benchmarking before deployment.
- **Data Quality:** Use validated, consistent, and relevant datasets. Avoid overfitting or data snooping.

3. Board and Senior Management Oversight

- **Model Risk Reporting:** Periodic reporting to the Risk Management Committee (RMC) on:
    - Inventory and status of models
    - Validation results and performance trends
    - Material model issues and mitigations

H. Information Technology Risk (IT Risk)

IT Risk, or Information Technology Risk, refers to the potential for loss or disruption resulting from inadequate, failed, or compromised IT systems, infrastructure, processes, or services. For an NBFC-MFI, IT Risk can significantly affect service delivery, data integrity, customer trust, regulatory compliance, and business continuity. RMC shall take regular inputs from the ITSC related to the IT Risk.

1. IT Governance and Policy Framework

- **IT Policy:** Develop and implement a board-approved IT Policy covering IT infrastructure, data management, cybersecurity, vendor management, and user access.
- **Information Security Policy (ISP):** Incorporate RBI's *Master Directions on IT Framework for NBFCs*.
- **IT Steering Committee:** Establish an internal committee responsible for IT strategy, risk monitoring, and investment decisions.

2. IT Infrastructure Risk Management

- **Hardware Redundancy:** Use failover servers, backup power supplies, and redundant network connectivity.
- **Software Controls:** Deploy licensed, patched, and updated software applications.
- **System Hardening:** Secure servers and endpoints with firewall, antivirus, and anti-malware tools.

3. Cybersecurity Risk Controls

- **Firewall & Intrusion Detection:** Deploy next-gen firewalls and intrusion prevention systems.
- **User Access Management:**
  - Role-based access controls (RBAC)
  - Multi-factor authentication (MFA)
  - Timely deactivation of ex-employee access
- **Regular Penetration Testing & Vulnerability Assessment (PT/VA):** Conduct periodic audits by independent agencies.
- **Security Information and Event Management (SIEM):** Real-time monitoring and alerting for abnormal activity.

4. Data Management and Privacy Controls

- **Data Encryption:** Encrypt data at rest and in transit using industry standards
- **Data Localization:** Ensure compliance with data localization norms (especially for Aadhaar data under AUA/KUA).
- **Data Loss Prevention (DLP):** Implement tools to monitor, detect, and block data exfiltration.

5. Business Continuity and Disaster Recovery

- **Business Continuity Plan (BCP):** Ensure continuity of operations in case of IT failure or cyberattack.

- **Disaster Recovery (DR) Site:** Maintain an off-site or cloud-based DR site with periodic failover testing.
- **Regular BCP/DR Drills:** Conduct mock drills involving IT and operations teams.

6. Vendor and Outsourcing Risk Management

- **Third-Party Due Diligence:** Assess vendors for cybersecurity practices, compliance, and IT controls before onboarding.
- **Contractual Safeguards:** Include clauses on data protection, breach notification, audit rights, and business continuity in IT vendor contracts.
- **Ongoing Monitoring:** Review vendor performance and security practices periodically.

7. Change and Patch Management

- **Change Management Policy:** Documented process for testing and approving software and infrastructure changes.
- **Patch Management:** Ensure regular patching of OS, databases, and applications to mitigate known vulnerabilities.

8. IT Incident Management

- **Incident Response Plan:** A formal response plan for cyberattacks, outages, or breaches.
- **24/7 Helpdesk:** Establish a helpdesk or support system for quick resolution of IT issues.
- **Root Cause Analysis (RCA):** Conduct RCA of every major IT incident and report it to management.

9. Compliance and Audit Readiness

- **RBI Compliance:** Align IT practices with RBI's IT Framework, UIDAI, CKYC etc..
- **Internal and External IT Audits:** Conduct audits covering system controls, cyber hygiene, and compliance.
- **IT Asset Register:** Maintain an up-to-date inventory of hardware and software assets.

10. Awareness and Capacity Building

- **User Training:** Regular training for employees on cybersecurity hygiene (e.g., phishing, password safety).
- **Simulation Exercises:** Run phishing simulations and cyber-attack mock drills.

- **IT Staff Skill Development:** Encourage them to develop their skills on continuing basis.

11. Reporting and Oversight

- **Board-Level Reporting:** Periodic reporting of IT risks, major incidents, and audit findings to the Risk Management Committee or Board.
- **IT Risk Heatmap:** Maintain a heatmap of IT risks and track mitigation efforts.

I. Fraud Risk

Fraud Risk refers to the possibility of financial or reputational loss resulting from intentional acts of deception, misrepresentation, or concealment by internal or external parties. For an NBFC-MFI, fraud may occur at any stage of the credit or operational cycle and can involve employees, customers, intermediaries, agents, or third-party service providers.

Risk Mitigation Strategy

A. Governance and Oversight

- The Company adopts a **Zero Tolerance** policy towards fraud in any form and at any level.
- A **Fraud Risk Management Policy (FRMP)** has been implemented which was approved by Board of Directors and shall be reviewed annually by the Board.
- A centralized **Fraud Risk Register** shall be maintained, monitored by the Risk Management Committee (RMC), and updated based on emerging risks and incident learnings.

B. Preventive Controls

1. **Process-Level Controls:**
    - Segregation of duties (SoD) in all financial and operational processes.
    - Maker-checker validations and dual authorizations for critical transactions (e.g., disbursement, write-offs).
    - Mandatory system-based workflows to limit manual overrides.

2. **Customer Onboarding & KYC:**

    - Compliance with RBI and UIDAI-prescribed KYC/e-KYC norms.
    - Aadhaar-based biometric verification using AUA-KUA authentication.
    - Geo-tagging of field verification for borrower due diligence.

3. **Technology Safeguards:**

    - Use of secure and tamper-proof LMS/LOS with built-in audit trails.
    - Integration of fraud detection and analytics tools to flag suspicious patterns.
    - Automated reconciliation between loan systems and bank accounts.

C. Detection Mechanisms

- Implementation of **Early Warning Systems (EWS)** based on red flag indicators (e.g., abnormal cash collections, duplicate borrower records, backdated entries).
- Surprise audits and periodic branch inspections.
- Establishment of a **Whistleblower Mechanism** to anonymously report unethical or fraudulent activities.
- Advanced **data analytics** to detect anomalies and investigate fraud indicators.

D. Investigation and Response

- All suspected or reported frauds shall be investigated by a designated Team.
- **Root Cause Analysis (RCA)** to be conducted post-investigation with a focus on control lapses and process gaps.
- Disciplinary and legal action to be initiated in accordance with internal HR policies and applicable laws.
- High-value or complex cases may involve forensic audits through empaneled external experts.

E. Reporting and Escalation

- Fraud incidents shall be reported to Senior Management and the Risk Management Committee.
- All frauds above the threshold prescribed by RBI (currently ₹1 lakh) shall be reported as per **RBI's Master Directions on Frauds – Classification and Reporting**.
- Regular MIS to be submitted to the Board and RMC, detailing fraud trends, categories, financial impact, and control effectiveness.

F. Vendor and Third-Party Risk Management

- Pre-onboarding due diligence of vendors for operational integrity and compliance history.
- Inclusion of fraud liability, data protection, and investigation cooperation clauses in third-party contracts (wherever possible).
- Regular audits and control checks for outsourced functions and digital partners.

G. Awareness and Training

- Periodic training for all staff on fraud typologies, red flag identification, and reporting mechanisms.
- Awareness sessions for borrowers on safe borrowing practices and risks of engaging unauthorized persons/Ring Leadrers.
- Culture of ethics and integrity to be promoted through leadership communication and internal campaigns.

H. Cyber Fraud and Technology Controls

- Strong access control systems, including 2FA and role-based rights management.
- System security measures such as firewalls, antivirus, SIEM, and endpoint protection tools.
- Regular PT/VA testing and cyber drills to assess and improve readiness.

I. Monitoring and Review

- Regular assessment of fraud control effectiveness as part of the Company's Enterprise Risk Management (ERM) process.
- Annual review of the Fraud Risk Management strategy in light of new fraud trends, regulatory updates, and operational experience.
- Inclusion of fraud risk in internal audits, concurrent audits, and risk-based branch visits.

J. Insurance and Recovery

- Appropriate **fidelity insurance** shall be maintained to cover losses from fraud-related incidents.
- Recovery of loss through legal action, insurance claim, and forfeiture of dues from involved employees or third parties shall be pursued.

This section shall be read in conjunction with the Company's Whistleblower Policy, IT and Cybersecurity Policy, and the Fraud Reporting Guidelines issued by RBI and other regulatory authorities.

J. Physical Risk

Physical Risk refers to the potential for financial loss, operational disruption, or reputational damage due to the direct impact of environmental, climate-related, or external physical events. These risks arise from Robbery, fire, natural disasters, extreme

weather, infrastructure failures that can affect the physical assets, staff, branches, and customer operations of an NBFC-MFI.

Risk Mitigation Strategy

A. Governance and Risk Assessment

- Physical risk management forms a part of the Company's **Operational Risk Framework** and is monitored by the Risk Management Committee (RMC).
- Periodic **site-level risk assessments** shall be conducted to identify vulnerable branches or field zones, particularly in geographies prone to natural calamities or unrest.

B. Infrastructure and Asset Protection

1. **Office and Branch Security:**
    - Controlled access to server rooms, record rooms, and cash safes.
    - Use of biometric or card-based access control for sensitive areas.
2. **Fire and Electrical Safety:**
    - Deployment of **fire extinguishers**, smoke detectors, and emergency exits at Head Office.
    - Periodic electrical safety audits and maintenance of wiring and equipment.
    - Fire safety training and evacuation drills for all staff.
3. **Cash Handling Risk Mitigation:**
    - Secure vaults, dual custody of keys, and tamper-proof cash bags.
    - Daily cash reconciliation and surprise cash audits.

C. Natural Disaster Preparedness

- **Disaster Preparedness Plans** to be developed at branch level, especially for locations exposed to floods (if any).
- Data and asset protection through offsite/cloud backups and document digitization.
- Mapping of alternate locations or nearby branches for temporary relocation in case of calamity.

D. Employee and Field Staff Safety

- **Field Visit Protocols**:
    - Geo-tagging of visits and check-in/check-out systems.
    - Mandatory reporting structure and emergency escalation protocol.
    - Avoidance of field visits during local unrest or in unsafe hours.
- **Safety Training**:
    - Awareness sessions on road safety, emergency response, and basic first aid.
    - Dedicated helpline number or local emergency contact for field staff.
- **Insurance Coverage**:
    - Group accident insurance and health cover for employees, including field teams.

E. Physical Record and Asset Protection

- Secure storage for physical loan files, agreements, and statutory records with access control.
- Digitization of key documents and secured upload into centralized systems.
- Regular asset verification and tagging of fixed assets with location and user mapping.

F. Civil Unrest and Law & Order Disruption

- Monitoring of local intelligence and news alerts for politically or socially volatile regions.
- Temporary suspension of operations or rerouting of staff if significant unrest is reported.
- Coordination with local authorities and law enforcement in emergencies.

G. Business Continuity Measures

- Integration of physical risk scenarios into the **Business Continuity Plan (BCP)**.
- Availability of backup power (inverter/generator) and alternate internet connectivity.
- Data backup, remote access readiness, and alternate work arrangements during crises.

H. Monitoring and Audit

- Inclusion of physical risk parameters in internal audits and operational risk reviews.
- Reporting of all physical incidents (fire, theft, damage) to Risk Cell and RMC with RCA and mitigation steps.
- Key risk indicators (KRIs) to be tracked – such as number of security breaches, incidents reported, loss events, etc.

This section shall be read in conjunction with the Company's Business Continuity Policy, Fire Safety SOP, and Employee Safety Guidelines.

K. Socio Political Risk

Socio-Political Risk refers to the potential for financial, operational, or reputational losses resulting from changes in the socio-political environment, including government policies, political instability, civil unrest, regulatory shifts, or public sentiment. For NBFC-MFIs, such risks are particularly relevant given their grassroots presence, reliance on community engagement, and sensitivity to local and regional political dynamics.

Risk Mitigation Strategies

A. Risk Identification and Assessment

- Regular monitoring of **socio-political developments** across operational geographies, especially in rural and semi-urban areas.
- Mapping of **sensitive and high-risk zones** based on historical incidents of unrest, elections, agitations, or community-driven disruptions.
- Inclusion of socio-political risk parameters in **branch-level risk assessments** and strategic expansion planning.

B. Operational Risk Mitigation Measures

1. **Location Diversification:**
    - Avoid excessive concentration of operations in politically volatile regions.
    - Diversify branch network across states and districts to reduce systemic exposure.
2. **Dynamic Field Operations:**
    - Real-time instructions to field teams in case of protests, hartals, local curfews, or regional shutdowns.
    - Postponement or rerouting of recovery, disbursement, or collection activities in high-tension zones.

3. **Local Community Engagement:**
    - Proactive engagement with local leaders, SHG heads, and community representatives to build trust and pre-empt hostility.
    - Financial literacy and awareness programs to address borrower concerns and reduce misinformation.

C. Regulatory and Policy Risk Mitigation

- Constant tracking of regulatory changes (RBI, State Governments, Local Authorities) that may affect interest rates, recovery mechanisms, or credit policies.
- **Policy Impact Assessment** for new government schemes, waivers, or moratoriums.
- Active participation in **industry forums** (like MFIN, Sa-Dhan) for representation and early alerts on policy changes.

D. Communication and Crisis Management

- Establishment of a **Crisis Communication Protocol** for timely and transparent communication with staff, borrowers, and stakeholders during unrest or politically sensitive events.
- Pre-approved communication templates for:
    - Public clarification
    - Temporary service suspensions
    - Employee advisories
- Appointment of **zonal escalation officers** to handle local issues swiftly.

E. Employee and Asset Safety

- Suspension of operations during elections, violent protests, or major political rallies as a preventive measure.
- Deployment of private security where physical risk is high.
- Insurance cover for property damage and staff injury arising out of civil disturbance.

F. Business Continuity Planning (BCP) Integration

- Include **socio-political disruptions** as a defined scenario in the BCP framework.
- Identify alternate sites or digital-first solutions for temporarily affected branches.
- Use of mobile-based customer service and tele-recovery during politically sensitive periods.

G. Monitoring, Reporting, and Governance

- Maintenance of a **socio-political risk log** capturing incidents, actions taken, and lessons learned.
- Periodic reporting of socio-political developments to the Risk Management Committee.
- Integration of socio-political risk into the **Enterprise Risk Dashboard** with KRIs such as:
    - Number of disruptions due to external unrest
    - Collection impact from local protests
    - Employee safety incidents reported

L. Other Risks may be identified from time to time by Management and can be reviewed and monitored by Risk Management Committee.

This policy, list of risk and mitigation plans and status can be read along with the Risk Matrix under Hazard Identification and Risk Assessment (HIRA).

ANNEXURE 1

RISK MANAGEMENT

Three Lines of Defence

Third Line of Defence
Internal Audit

- Validate the overall risk compliance and central framework
- Provides assurance that the risk management process is functioning as designed

Second line of Defence
Compliance department

- Establishment standards for compliance
- Independently monitor compliance
- Develop and maintain policies and procedure
- Report non-compliance of regulation & direction to Senior Management
- Design and develop overall risk management framework independly across the organisation
- Monitor corporate and business unit
- Adherence to framework and strategy

First Line of Defence
Business unit i.e. Branches

- Owns the risk management process
- Identifies, Manage, mitigates and report on risk
- Track losses, incidents data

ANNEXURE 2

Risk Inventory

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Risk Number	**Risk Short Name**	**Risk Description**	**Existing Risk Controls/Measures in Place**	**Outcome**	**Impact**	**Likelihood**	**Impact Score**	**Likelihood Score**	**Net Score**	**Risk Mitigation Action**	**Responsibility**	**Cost Estimation**	**Resources needed**	**Target date for completion of mitigation plan**
1	Risk #1													
2	Risk #2													
3	Risk #3													
4	Risk #4													
5	Risk #5													
6	Risk #6													
7	Risk #7													
8	Risk #8													

Scoring the Risk

Impact	**Score**	**Likelihood**	**Score**
Critical	5	Expected	5
Serious	4	Highly likely	4
Moderate	3	Likely	3
Minor	2	Not Likely	2
Insignificant	1	None/Slight	1

****

Digamber Capfin Limited

Address: J 54-55, Anand Moti, Himmat Nagar, Gopalpura, Tonk Road, Jaipur-302018, Rajasthan.