CreditAccess Grameen Limited

RISK MANAGEMENT POLICY

Version control

Version	Date	Type of change	Author	Reviewer
8.0	Oct 25, 2024	Policy Approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD
7.0	June 25, 2024	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD
6.0	April 01, 2024	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD
5.0	May 16, 2023	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD and CEO
4.0	May, 2022	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD and CEO
3.0	June 25, 2021	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD and CEO
2.0	Nov 06, 2020	Policy approved by the Board	Firoz Anam Chief Risk Officer	Udaya Kumar MD and CEO
1.0	Jan 12, 2018	Policy approved by the Board	Gururaj Rao Chief Audit Officer	MD & CEO

Summary of Changes from Version 7:

Sl. No.	Section	Page No	Description of Change
1	3.4, 8	7, 22	New Product Approval Committee added
2	6	18	New section on fraud risk management added in line with RBI regulation

CONTENTS

1. Introduction

Credit Access Grameen Limited ("Company") is one of the leading microfinance institutions in India focused on providing financial support to women from low-income households engaged in economic activity with limited access to financial services. The Company predominantly offers collateral free loans to women from low-income households, willing to borrow in a group and agreeable to take joint liability. The wide range of lending products address the critical needs of customers throughout their lifecycle and include income generation, home improvement, children's education, sanitation and personal emergency loans. In 2016, with a view to diversifying the product profile, the company introduced individual retail finance loans for customers who had been the customers of the Company for at least three years. These loans are offered to customers, for establishing a new enterprise or expand an existing business in their individual capacity.

The purpose of the risk management policy is to provide guidance on identifying, managing and mitigating risks arising across risk taking activities in the organization to ensure sustainable profitability. The policy applies to activities and processes associated with the normal operations of the organization and covers areas such as credit risk, reputation, technology, funding, operations, regulatory, strategy, etc.

The risk architecture will support our Company's vision to to be the preferred business partner of Indian households lacking access to formal credit, enriching their lives by providing convenient and reliable solutions, matching their evolving needs. Following are the basic building blocks of risk management structure:

- **Risk appetite and strategy:** Risk appetite clarifies the risks that the organisation is prepared to accept and manage in the pursuit of its objectives and those which it does not. The statement provides the boundary conditions of risk along with the go/no-go areas.
- **Organisation structure and governance:** Organisation structure and governance framework shall ensure independence of the risk function while providing sufficient oversight and effective challenge. Organisation structure shall be in line with the three lines of defence model with focus on identifying and mitigating new age risks such as cyber risk.
- **Credit risk assessment and risk analytics:** Analytics shall be embedded directly into making decisions, taking action and delivering value to various stakeholders. Analytics shall deliver agility and ensure test and learn on tools and models for developing holistic customer view (including risk assessment, customer lifetime value, etc.).
- **Risk controls, monitoring and reporting:** Effective monitoring process with early warning signals and feedback mechanisms in underwriting policies shall be in place. Operational risk controls shall have a feedback loop into new product development. Internal reporting process shall ensure adequate oversight with the support of actionable dashboards.
- **Systems and data:** The organization shall take concrete steps to build internal data, gather external and alternate data while ensuring proper data quality. The systems and IT infrastructure shall enable scalability and agility.
- **Risk culture:** CA Grameen shall strive to build and embed a common organisation culture with shared goals and objectives. The organisation shall focus on building a healthy risk culture by linking performance to risk and capital metrics.
- **Role of risk in management of business:** Risk shall be active in a broader range of areas such as capital planning and budgeting, solvency, liquidity and funding, product design and pricing, etc. and play the role of challenger and advisor to the business.

2. Risk appetite:

Risk appetite is one of the most important components for coordinating the risk-taking activities across the organisation and provides the boundary conditions of risk along with the go/no-go areas.

In order to clearly define the company's credit appetite as well as acceptable level factoring risk-reward trade off, the company has put in place threshold (viz entry level credit bureau checks for fresh as well as incremental exposure) for considering all credit proposals.

As CA Grameen expands its business, core high-level statements shall guide the organisation on the risks that it should be prepared to accept and manage in the pursuit of its objectives and those which it should not.

2.1 Risk appetite statement:

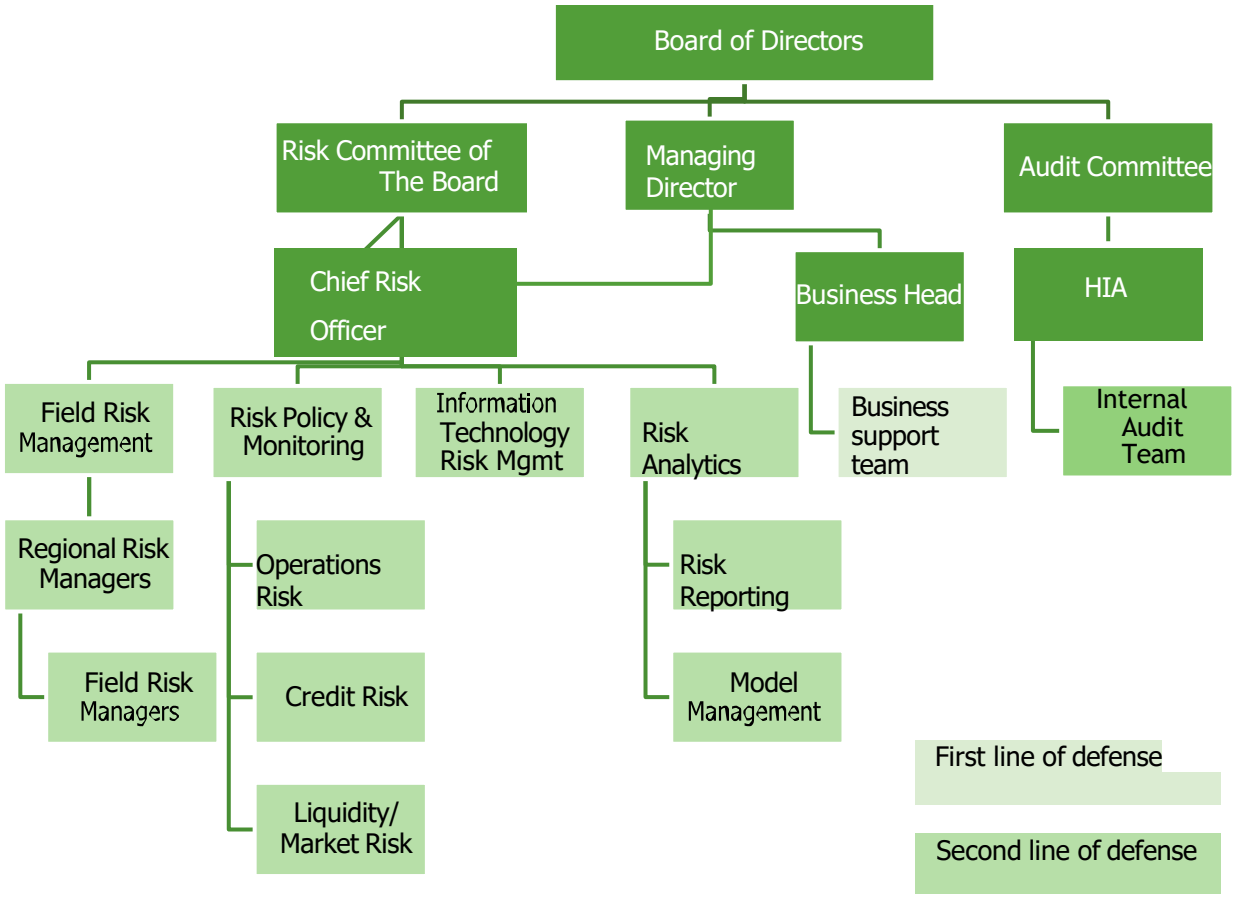
Overall, CA Grameen's risk appetite is low to moderate. Maintaining relatively tight caps on risk exposures is seen as the most conducive approach to providing cost-appropriate mass-market financial services in a socially inclusive manner. CA Grameen rejects any speculative approach to financial services delivery. The corner stones of CA Grameen's business model are customer service, outreach and financial inclusion, innovation, technology, proactive risk management and sustainable growth. For example, CA Grameen will not engage in activities, trade instruments or otherwise enter into risks that do not have a clear relationship to the mission of the institution and support CA Grameen in delivering on its promise to shareholders and customers of integrity, social advancement, economic empowerment and sustainable profitability. This stated mission and fundamental risk appetite will guide CA Grameen in developing its strategy, in considering decisions about new products or new markets and in setting appropriate exposure limits in each of the risk areas.

In addition to this statement, the risk appetite framework includes a set of quantitative bounds on the acceptable levels of risk.

3. Risk Governance Structure

CA Grameen shall follow a three line of defense mechanism in which the business line including branch & supervisory staff and business support team work as first line of defense. Risk Management is the second line of defense while Internal Audit works as the third line of defense. The management of risks is not confined to the Risk Manager and the dedicated risk management department. It is a responsibility of all senior management and of all staff in all business lines. Each line of business is responsible to manage its own risks.

The CRO has primary responsibility for overseeing the development and implementation of the CA Grameen's risk management function. The CRO is responsible for supporting the board in the development and implementation of the CA Grameen's annual risk plan. In addition, CRO is responsible for supporting the board in its development of CA Grameen's risk appetite and for translating the risk appetite into a risk limits structure. The CRO, together with management, should be actively engaged in the process of setting risk measures and limits for the various business lines and monitoring their performance relative to risk-taking and limit adherence. The risk organization structure is provided below:



3.1 Board Committee Structure

The Risk Management Committee shall have minimum three (3) members with majority of them being members of the Board of Directors, including at least one Independent Director.

3.2 Meetings and Quorums

The Risk Management Committee shall meet quarterly in a financial year.

The quorum for meeting of the Risk Management Committee shall be either two Members or one third of the Members of the Committee, whichever is higher, including at least one Member of the Board of Directors in attendance.

The Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if considered necessary.

3.3 The roles and responsibilities of Risk Management Committee

Roles and responsibilities of Risk Management Committee inter-alia, includes the following:

- To ensure that appropriate methodology, processes, and systems are in place to monitor and evaluate risks associated with the business of the Company.
- To assess the Company's risk profile and key areas of risk in-particular

- To approve CA Grameen's annual risk plan and monitor its implementation.
- To examine and determine the sufficiency of the Company's internal process for reporting on and managing key risk areas.
- To assess the changes in the Company's risk profile and assess specific risks and adequacy of the risk management process.
- To review the monitoring updates and actions taken as reported by the Management Level Risk Committee
- To approve the credit risk policies related to individual products.
- To approve any other specific risk policy e.g., financial risk management policy, operational risk management policy
- To monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems.
- To keep the Board of Directors informed about the nature and content of its discussions, recommendations, and actions to be taken.
- To review the appointment, removal, and terms of remuneration of the Chief Risk Officer.

3.4 Management Committees:

a. New Products Committee ("NPC") – Committee shall comprise of CEO, CRO, COO and CCO. The Committee (NPC) shall oversee and approve all new products proposed to be introduced by the Company.

b. Management Level Risk Committee (MLRC) comprises of MD, CEO, COO, CFO, CTO CCO and CRO. The department heads will be accountable to the MLRC for identification, assessment, aggregation, reporting and monitoring of the risk related to their respective domain.

Accordingly, the Management Level Risk Committee would review the following aspects of business specifically from a risk indicator perspective and suitably record the deliberations during the monthly meeting.

- Review of business growth and portfolio quality
- Discuss and review the reported details of PAR, Key Risk Threshold breaches (KRIs), consequent responses and operational loss events.
- Breach of process compliances leading to enhanced risk
- HR management, training and employee attrition
- Impact of new product/policy/process changes
- Performance of IT systems and their integration with existing IT structures, including extant IT Policy
- Escalation of risks which have substantial impact to the business and meet determined escalation threshold levels to the relevant Department.
- Review the status of risks and treatment actions with key staff in their respective areas. Any new or changed risks will be identified and escalated, if deemed necessary. Particular emphasis is to be given to risks with high ratings and their corrective actions.

3.5 Roles and responsibilities of risk function:

Risk function shall assess and understand the risks at an enterprise level to identify where the organisation is exposed. Risk function shall be responsible for identifying, articulating, monitoring, and measurement of risk at an enterprise level including credit, market, operational and other non-financial risks, cyber risk and other emerging risks. Key activities of the risk management function should include:

- Identifying material individual, aggregate and emerging risks

- Assessing these risks and measuring CA Grameen's exposure to them

- Supporting the board in its implementation, review and approval of the enterprise-wide risk governance framework which includes the CA Grameen's risk culture, risk appetite and risk limits.

- ongoing monitoring of the risk-taking activities and risk exposures to ensure they are in line with the board-approved risk appetite, risk limits and corresponding capital or liquidity needs (i.e., capital planning)

- establishing an early warning or trigger system for breaches of the CA Grameen's risk appetite or limits.

- influencing and, when necessary, challenging material risk decisions; and

- reporting to senior management and the board or risk committee, as appropriate, on all these items, including but not limited to proposing appropriate risk-mitigating actions.

The risk management function does not replace the business line's responsibility (first line of defense), but rather enhances it by monitoring and analyzing risks, recommending risk management strategies, and preparing stress tests and scenario plans. The Risk Function must work with all departments within the Company. Whereas each department focuses on its specific area of activity, the Risk Function operates in cooperation with all departments in order to improve the management of corporate risks following the guidelines approved by the Risk Committee of the Board

The CRO who is the Risk Head shall oversee the following functions:

a) Credit Risk function (Section 4):

- Define & maintain credit policies, standards, delegation framework.
- Design, maintain, monitor and report early warning signals.
- Monitor portfolio quality & trends.
- Forecasting of credit loss

b) Operational Risk function (Section 5):

- Field risk management of operational centers
- Operational risk measurement, monitoring and report, limit setting
- Maintain RCSA framework i.e. identify all risks that are not captured in the standard risk frameworks.
- Advise new product development on operational risk aspects.
- Incident/Fraud monitoring & reporting
- Involve and support in investigation, route cause analysis etc., and suggest mitigations.

c) Liquidity/Market Risk function (Section 6):

- Funding Risk metrics development and monitoring

- Interest Rate/Currency risk metrics/models development and monitoring
- Liquidity risk metrics development and monitoring
- Stress Testing / Scenario Analysis with respect to Liquidity/Interest Rate/Currency Risk

d) Information Technology Risk function (Section 7):

- Information Risk framework and policy
- Methodology and process for cyber risk assessment
- Independent assessment of risk across all information asset

e) New product assessment approval (Section 8):

- Risk assessment related to new products.
- Vetting of policies and processes

f) Risk Analytics and Model management function (Section 9):

- Development of Risk Models
- Validation of Internal/external Risk Models

3.6 The Role of the Audit Committee and Internal Audit

The Audit Committee's responsibilities are the oversight of financial reporting and disclosure, as well as monitoring the effectiveness of the internal control process and of the internal audit function. The AC also get involved in issues of regulatory compliance and dealings with external auditors. Through its direct access to the Board and through its oversight of the Independent Audit function (the **"third line of defense"**), the Board Audit Committee plays a critical role in the risk governance framework.

Internal Audit (IA) is a systematic continuous appraisal of an Institution's operations/processes and financial reports (it is an integral part of the overall risk management process). In relation to the second level of controls carried out by the risk management function, IA performs the third level controls including assessing the correct implementation of the RM policies. IA is independent and reports directly to the Audit Committee of the Board.

It is undeniable that it is important to strengthen the relationship between 2nd and 3rd line of defence (risk and audit functions):

- The synergy between the two teams will help management (and Board) to get a clear idea of critical areas, as well as areas to be exploited as opportunities.
- Linking risk assessment with the risk-based annual audit plan is perhaps one of the most effective ways to ensure collaboration.

4. Credit Risk Management

a. Principles of credit risk management

As a micro finance company (MFI), CA Grameen is prone to significant credit risk. Credit risk is the largest source of risk and hence a specific focus on identification, measurement, monitoring and mitigation of credit risk is important.

Definition:

Credit Risk is defined as the possibility of losses associated with diminution in the credit quality

of borrowers. In company's portfolio, losses stem with outright default due to inability or unwillingness of a customer to meet commitments in relation to lending. Alternatively, losses result from reduction in portfolio value arising from actual or perceived deterioration in Credit quality.

b. Credit Risk Management Strategies

- The company shall ensure the required expertise and capability to develop systems, procedures and tools to effectively manage the credit risk are provided for.
- The company shall also develop the skills and capabilities of associated staff in the process of measuring, monitoring and controlling Credit Risk and thus implement the tool/model in the organization.
- The company shall specify the acceptable level of risk-reward trade-off for its various products and activities where monies are exposed to Credit Risk. This would necessarily translate into the identification of target geographies/markets and business sectors, preferred levels of diversification and concentration, the cost of capital in granting credit and cost of bad debts.
- In the credit policy it will be addressed by way of deciding the thrust and restricted areas of lending, statutory, and regulatory restrictions, exposure norms, criteria of lending etc.
- Risk Management Guidelines issued by RBI shall continue to act as a guiding factor while formulating and implementing the risk system in the company. The company shall continue to comply with all statutory and regulatory guidelines/ restrictions as stipulated by RBI, MFIN, SADHAN etc. from time to time.
- Keeping in view the performance of different products/geographies/segment and the risk perceived in the segment, the company shall define exposure ceiling for aggregate commitments to specific geographies/ products/ segments, categories of borrowers etc.
- Company has defined delegated power of officers in various designations (BM /AM/Divisional or Zonal/ Business Head) for sanction of credit proposals. Based on risk profile and other factors, delegated power for loan advances is reviewed by the Board of Directors from time to time.
- Company shall ensure geographical concentration limits as specified in company's risk appetite statement / document.

c. Credit appraisal process:

Sourcing, credit, and risk will be involved in various steps of the end-to-end credit process.

i. <u>Sourcing of business:</u>

Sourcing is the first step of credit process, and a well sourced business shall enhance portfolio quality and returns while containing the PAR. The company shall source business by leveraging the network of branches and Kendras. The company shall also strive to add new Kendra and branches in potential locations.

The organisation shall select creditworthy clients through checks and verifications at the time of inception. The salesforce shall target customers keeping in view the following aspects:

- The customer groups are well within the stipulated distance from the branch (in case of opening of new Kendra)
- There are no adverse signs of potential interference in the business-like anti MFI/banking political movements, previous large-scale customer frauds, high PAR rates and apparent willful default by members.
- Expected profitability from the target customers.

- Successful completion of Group Training and clearing GRT.
- Satisfactory infrastructure availability

Risk Management may issue additional guideline from time to time with respect to customer sourcing that will be incorporated into the sourcing policy and procedure.

ii. Credit assessment, approval and disbursement:

Credit appraisal would be in conformity with respective product level credit policy and would be subject to necessary due diligence for ensuring consistency in quality and adopting uniform credit standards. Credit appraisal process will typically include the following steps:

- **Eligibility check**: Basic checks to ensure that an application / proposal satisfies the boundary conditions and having a Credit Bureau from CIR
- **Verification**: Physical verification where required including identity, address and property.
- **Assessment**: Detailed assessment based on a set of parameters which will determine the loan conditions such as income, loan purpose, prior repayment history etc. as per the product.
- There shall be a list of negative profile (product specific and/or general) that will include Prohibited Investment Activities List (PIAL). The PIAL shall be maintained as part of ESG Governance policy. Appropriate due diligence shall be undertaken to ensure that no business falling under PIAL is funded by CA Grameen.
- The credit proposal to be processed at the Appropriate delegated authority.
- Disbursement after thorough checking of the identity of the borrower in physical form
- Disbursement to be made after appropriate consent has been obtained from the borrower.
- All the terms and conditions along with the details such as interest rates, EMI, insurance, taxes, processing fees etc., to be explained in advance to the customers.
- The competent authority will necessarily visit the site of business after disbursal and monitor the end use of funds.

d. Collection and Recovery

Collections to be made against particular account as per provisions of each product line.

- For GL collection primarily to be made in the Kendra Meeting, while for RF the collection should mostly occur through direct debit to customer bank account as per authorization received. However, customers shall be allowed to make payments through electronic mode such as BBPS & UPI.
- The practice of accurately recording the received cash against correct account with correct balances
- The collections received in cash to be entered into the core solution within the stipulated timeframe.
- Remitting the cash balance received to the attached bank account/ branch in the shortest possible time.
- Reconciliation of entries and mismatches at different functional levels in the organisation
- Ensuring a robust MIS and reconciliation system in place which can eliminate/ minimise any operational risk in the collection process.
- To be ensured that the staff involved in collection process follow all relevant procedure according to the Client Protection Principles and fair practices code of RBI.

e. Monitoring and reporting:

Effective monitoring process with early warning signals and feedback mechanisms in underwriting policies shall be in place.

i. Credit monitoring:

The organisation will classify accounts in alignment with statutory requirements. In addition, the organisation would also identify special mention accounts based on state of delinquency. CA Grameen shall monitor these stressed accounts and minimize the slippages to NPA using following measures:

- Tracking of overdues intensively.
- Frequent interaction with borrower/regular visits.
- Discourage additional exposure to these accounts under delinquency management.

At the portfolio level, CA Grameen shall implement early warning signals to help take portfolio level strategic action for segments with signs of increasing stress and CA Grameen shall implement feedback mechanism to policy, underwriting and sourcing.

The purpose of the analysis is to isolate factors/sub-segments/micro-segments which are likely to influence the credit quality of the portfolio. As such, own portfolio analysis will be performed at various portfolio cuts such as state, branch, customer profile, sourcing channel, customer indebtedness etc.

The organization would review its exposures to form an opinion whether to grow, continue, reduce or exit for optimizing the risk vis-à-vis returns. Such reviews would be conducted on a selective basis before the MLRC Some of the factors which can be considered for forming a view are credit quality of the portfolio, developments in the MFI industry, etc.

ii. Internal and external reporting:

CA Grameen shall have actionable dashboards to regularly report portfolio quality to the top management. The dashboards shall include portfolio level summary with the ability to drill-down up to state/district/branch/kendra level. CA Grameen shall also comply with the regulatory reporting requirements including the Credit Information Companies (CICs) as recommended by RBI.

f. Collateral Management:

Presently the company deals majorly in non-collateral advances due to the nature of business. But recent venture into collateral backed products, to the permissible limits as per statutory guidelines, the company will obtain collateral in such business verticals to mitigate risk of lending to a borrower. The organization would follow the below guiding principles in management of these collateral:

- Title of Ownership must be clear, and it should be free of encumbrances.
- Valuations and legal due diligence must be done by trained staff /qualified valuers & lawyers
- Appropriate documentation must be created in a timely manner and maintained to ensure that charge created on the borrower's assets as security for the debt is maintainable and enforceable.

g. Roles and Responsibilities of Credit Risk Management

- The risk team is responsible for defining the credit policy with respect to individual products in consultation with the concerned business teams. Such policy shall be reviewed by Managing Director and approved by the Board.
- The business and operation/credit teams are responsible for sourcing of customer, carrying out due diligence with respect to customer, assess credit proposals, approve credit proposal and disbursal of loan.
- The operation teams shall be responsible for carrying out the collection & recovery activities.
- Legal & technical due diligence of collateral shall be carried out by the respective business and operations team.
- The risk team shall be responsible for monitoring of customer/portfolio, identify risk and communicate with the business on suggested measure to mitigate the risk.
- Any model used for assessing credit proposal shall be validated and approved by the risk team.
- The Internal Audit team shall be responsible for carrying out checks on adherence of policy & procedure.
- Internal audit shall give independent feedback in terms of control environment (including policy and procedures) gaps to the MD, CEO, CRO, COO and to the Audit Committee

5. Market and Liquidity Risk Management

This section sets out the broad policy framework for identification, measurement, monitoring and mitigation of critical market risks that will be faced by the organisation. As a microfinance company, CA Grameen will be prone to liquidity risk, funding risk, interest rate risk and foreign exchange risk.

a. Liquidity Risk

Liquidity risk is the inability of an organization to meet the current and future loan obligations to its customers due to uncertain liquidity. This could arise due to a range of reasons such as mismatch in the tenor of loan and funding sources, negative changes in the credit rating, market-wide liquidity event, delay in collections, etc. Any default on its obligations can lead to reputation risk and long-term business impact.

i. Liquidity buffer

Liquidity risk management shall involve maintaining sufficient liquidity buffer on a continuous basis to fulfil immediate obligations including debt repayment, disbursal on loans committed, etc. Basel III norms mandate sufficient liquidity to fulfil obligations over 30 days. CA Grameen shall set its own survival horizon for various liquidity scenarios and the same has been articulated in the Board approved ALM policy.

ii. Monitoring and reporting

Within each time bucket, there could be mismatches depending on cash inflows and outflows. While the mismatches up to 1 year would be relevant since these provide early warning signals of an impending liquidity problem, the main focus has to be short term mismatches i.e. 1 day to 30/31 days (one month). RBI has therefore advised NBFCs to monitor their cumulative mismatches across all time buckets and establish/ fix internal prudential limits for the time buckets. CA Grameen shall also adhere to these prudential limits and the tolerance/ prudential limits for structural liquidity under different time bucket as prescribed in the Board approved ALM policy.

b. Funding concentration risk

As a non-deposit accepting NBFC MFI, CA Grameen will be highly reliant on wholesale funding which will give rise to the risk of dependence on few funding sources. Therefore, in order to reduce concentration, CA Grameen shall set internal limits on the share of a single lender in CA Grameen's total borrowings. Risk (in consultation with treasury) shall define the boundaries of funding risk and monitor the relevant metrics. Risk shall monitor the risk arising out of non-renewal of credit facility from existing borrower. Further, CA Grameen shall make efforts to avoid covenant(s) that requires sharing proprietary information with a potential competitor.

c. Interest rate risk

Interest rate risk arises on account of interest rate related fluctuations, which could have a potential impact on earnings if the assets and liabilities have a mismatch on tenor or in the underlying rate fixing mechanism (fixed/floating linked to different benchmarks/combination with periodic resets). The loans made by the company carry fixed interest rate. On the other hand, the borrowings from bank/FI are in both fixed and floating. However, majority of the floating rate borrowing have 1 year rest against loan tenure of 2-3 years. As a result, the interest rate risk is significantly reduced. Nevertheless, procedure shall be developed to measure the extent of interest rate risk and monitored regularly by Risk in consultation with Finance department.

d. Currency Risk

Forex risk results from a mismatch between assets and liabilities in a currency and their associated cash flows in respect to size and maturity. CA Grameen may borrow in foreign currency from institutions abroad, but foreign currency exchange rates fluctuate over time. Such borrowing exposes the company to risk as CA Grameen's loan assets are in INR. Such risk can be mitigated by appropriate hedging strategy, or such risk may remain open if it is within acceptable limit.

It is not in compliance with the mission and mandate of CA Grameen to actively seek profit opportunities from speculative trading in foreign currency. CA Grameen is not authorized to maintain a proprietary trading book in short-term foreign currency instruments. Any foreign currency transaction must display a clear linkage to the client-related business.

CA Grameen shall not maintain any open foreign currency position, all foreign currency borrowing must be adequately hedged.

e. Roles and Responsibilities of Market & Liquidity Risk Management

- The Finance department is responsible for developing overall borrowing plan, investment strategy or mandate for the liquidity buffer and maintain contingency funding plan.
- The Finance department will be responsible to manage day to day cashflow requirement, mitigate it through changes to funding strategy and liquidity buffer, execute foreign currency hedging where applicable.
- The Finance department is responsible for taking appropriate measures to maintain the foreign currency risk exposure within specified limits at all times.
- Finance department is responsible to maintain compliance with respect to regulatory guidelines.
- The risk team is responsible for defining the methodology for liquidity/funding/currency/interest rate risk assessment in consultation with finance department.
- Risk team shall be responsible for monitoring early warning signal, conducting stress test / scenario analysis with respect to Liquidity/funding/currency /interest rate risk.

6. Operational Risk Management

6.1 Apart from credit and market risks which can be clearly defined, the organization also faces risks which can emanate from a range of sources including processes, people, systems, external events and can lead to substantial drag on earnings or threaten solvency in rare cases. This section sets out the broad policy framework for identification, measurement, monitoring and mitigation of operational risks. A separate section has been developed to outline the policy related to fraud risk management in Section 6.2

The major factors that drive operational risk inherent in CA Grameen are listed below,

Factor	Operational risks
People	1) Human errors during transaction 2) Employee driven frauds and misappropriation 3) Behavioral patterns that may have major reputational or legal implications. 4) Loss of key personnel
Process	1) Gaps in internal controls that may impact business 2) Higher dependence on manual intervention in day-to-day operations
Systems	1) Failure of software applications. 2) Security breaches (phishing, hacking, malware attack etc.) 3) Inadequate IT infrastructure.
External Events	1) Risk arising from third party intervention such as political entities, leading to willful defaults or frauds or business interruptions. 2) Damage to property and assets due to natural disaster, robberies, riots 3) Potential reputational and legal damage due to negative media coverage.

a. Management of operational risk

CA Grameen shall manage operational risk using the following methods.

i. Identification and Assessment of Operational Risk

CA Grameen shall identify and assess the operational risks inherent in activities, products, processes and systems across all business lines. In addition, CA Grameen will also conduct a top down risk assessment to identify the largest operational risks for the organization.

CA Grameen shall ensure that new activities, products, processes and systems are also assessed for operational risks at the time of launch. Operational risks associated with change initiatives shall also be assessed and managed.

Top risk events shall be prioritized based on frequency, ease of detection and severity. The following methods shall be adopted to identify and assess operational risk:

- **Risk and control self-assessment (RCSA)**: As the organization matures and reaches critical size, CA Grameen shall develop the RCSA process for identifying, assessing and evaluating risks in a consistent format across various processes, activities, systems, etc.

Risk function shall define the RCSA framework which will cover the methodology for assessing inherent and residual risk as well as the action plans for risks and controls which are outside tolerance level.

- **Key risk indicators**: Key risk indicators (KRI) shall be defined and regularly monitored by the risk function.
- **Loss event management:** Internal and external loss events shall be captured and reported on a regular basis to realise the impact. Loss events will also be reported through KRI and RCSA dashboards to monitor impact on specific controls or metrics. The type of major loss events would include frauds and misappropriations, personal transactions, robberies, business disruptions and system failures, damage to physical assets, loss arising due to failed execution of processes or products.
- **Scenario analysis**: CA Grameen may develop scenarios for low frequency but high impact potential loss events such as natural calamities, political events etc. Scenario analysis shall focus on developing the scenario narrative and quantification of scenario impact.

ii. Mitigation, Monitoring and reporting

CA Grameen shall ensure efficacy of controls for operational risk. This shall include internal controls, training, insurance, fraud monitoring, IT systems and security, business continuity planning, etc.

As part of risk and control self-assessment (RCSA), KRI dashboards shall be designed for major business lines (Finance & Accounts, IT, HR, Centralized Operations, Business teams), which will support in monitoring key risks and their underlying controls. Consequently, improved controls shall be recommended to decrease residual risk.

b. Roles and Responsibilities of Operational Risk Management:

- The individual departments shall be responsible for carrying out RCSA, identify Key Risk Indicators (KRIs), set appropriate limits, monitor KRIs, formulate action plan in consultation with the Risk team.
- The risk team shall monitor the implementation of action plan with respect to KRIs that are in breach of set limit.
- The Risk team shall ensure that management level KRIs are presented before the MLRC.
- MLRC shall review the management level KRIs and review action taken report where there is a breach of limit.
- Identification of Fraud/other incidents to be done by all operational teams. Internal Audit and Risk may also identify incidents of fraud /other incidents.
- Risk team shall be responsible for reviewing incidents, identifying root cause and suggest remedial steps. Risk team shall monitor the closure of open incidents.

iii. Field Risk Management

The field risk Management team is an extended arm of the risk management function. They form the critical link between the corporate office and the field. The team monitors that policies/ procedures are transmitted to the field and identify the risks and report the same back to risk

management department at HO.

a. Monitoring and management of field risk

Key risks in the field shall be monitored and controlled using the following methods:

- **Field Risk Surveys –** The field risk management team shall monitor key operational risks at branches and Kendra's through field risk profile questionnaires. The responses will consequently be used for reporting potential risks with respect to stakeholders at the branch and Kendra levels.

- **Fraud and PAR investigation –** The field risk team shall conduct investigation of frauds and PAR events in field, assess gaps in underlying controls and recommend improvement in controls.

- **Risk assessment of new proposed locations –** Prior to branch expansion in the organization, vetting of branch expansion proposals and geographical risk assessment of locations shall be conducted by assessing major operational and credit risks in the proposed locations.

b. Roles and Responsibilities of Field Risk Management

- Monitoring of operational risks at branches and Kendra's through field risk profile Questionnaires.
- Investigate delinquency/fraud events in branch or geographical area with high incidents being reported.
- Examines any risk events (Social, Political, PAR, Frauds, Culture, Ring Leaders/Agents issues etc.) that occurred in the region.
- Conducts Fraud/other incident Investigation and identify root cause in consultation with the respective department(s).
- Identify external risks including third party interventions and escalate to concerned stakeholders.
- Ascertains client protection principles are followed during employee/customer interactions.
- Capture and report the perception of local community towards CA Grameen.
- Collating the risk incidence information across branches within his/her purview.
- Conduct geographical risk assessment for business expansion when required.

iv. Business Continuity Planning

CA Grameen, like any other institution, is exposed to numerous operational risks that threaten to disrupt critical business operations. Thus, it is important to have a business continuity plan (BCP) that can be implemented during the time of an unplanned incident, so that all critical operations can continue to be performed.

CA Grameen shall have a business continuity plan that primarily includes:

- Description of scenarios during which BCP will be triggered.
- Risk assessment containing the threat scenario and response to each threat.
- Documentation of necessary resources required to perform the BCP.
- Details of officials responsible for managing BCP scenario.

a. <u>Response at HO</u>

The critical tasks that are expected to be performed at head office in case of a disruptive event are given below. The response is not limited to the following tasks:

- Managers should ensure that all arrangements are made for their teams to work remotely if required.
- Ensure functionality of all critical systems such as servers, applications etc. and other critical services at the workplace.
- Ensure all business reports, risk reports, incident reports, forecast reports etc. are sent regularly to management and board of directors.
- Regularly review the impact of ongoing disruption and develop recovery strategies accordingly.
- Maintain constant and effective communication.

b. Response in field

The critical tasks that are expected to be performed in the field (branch, regional and divisional offices) in case of a disruptive event are given below. The response is not limited to the following tasks:

- Managers should ensure that all arrangements are made for their teams to work remotely if required.
- Ensure functionality of all critical systems such as servers, applications etc. and other critical services such as access to IT support.
- Managers should identify staff with critical roles and which staff can work from home. They should also identify transferable skills to ensure smooth functioning of operations.
- Review staffing arrangements and temporarily deploy staff from other areas, if required.
- Report major incidents occurring in the field that may impact the organization.
- Maintain constant and effective communication at all levels.

Roles and Responsibilities

- The risk management team shall prepare a BCP as described in section 6(d) and update the document periodically.
- The individual departments shall be responsible for identifying necessary resources required to perform those functions.
- The individual departments shall ensure that the plan will work properly during a disruptive event. Most cases this will require staff access to remote work facility. However, in certain cases (e.g. IT Infrastructure) additional testing may be conducted on a regular basis.

6.2. Fraud Risk Management

The fraud risk management policy has been formulated in line with RBI Fraud Risk Management in NBFCs Directions 2024.

6.2.1 Governance Structure on Fraud Risk Management

- There will be a Special Committee of Executives for Monitoring and Follow-up (SCEMF) of cases of fraud comprising of MD, CEO, CRO and COO. The committee shall assess the progress of fraud cases periodically (at least quarterly) and place the progress report before the board annually
- There shall be a fraud risk management function headed by a senior official to be setup within the risk management function
- Risk Management function shall be responsible for prevention, early detection, investigation, staff accountability, monitoring, recovery, analysis and reporting of frauds

6.2.2 EWS Framework for Fraud Risk Management

- The company shall have a EWS system that shall identify early warning indicators for monitoring activities in the loan accounts. Suspicion of fraudulent activity thrown up by

one or more EWS indicators shall alert / trigger deeper investigation from potential fraud angle

- The EWS system must be comprehensive and designed to include both quantitative and qualitative indicator as appropriate for the product
- Risk Management Committee (RMC) of the board shall oversee the effectiveness of the EWS. A report on effectiveness of the indicators shall be placed before the RMC for this purpose
- The company shall continuously try to upgrade the EWS system through designing new type of indicators and adding new source of information where possible
- The risk analytics units shall monitor and analyze digital transactions to identify unusual pattern

6.2.3 Staff Accountability

- Fraud can be detected either by business teams or by the monitoring teams. Upon detection investigation shall be carried out by the risk team in consultation with business support team
- On conclusion of the fraud investigation at field, a report shall be issued by the investigation team. If any employee involvement is suspected, it will be intimated to the HR to issue show cause notice (SCN) to the concerned employee
- A reasonable time of 21 days or more shall be provided to the accused employee to respond to the SCN
- Once the response if received, the matter would be referred to the Disciplinary Committee on fraud / financial misappropriation investigation (FIC)
- Depending on the response, the FIC may call the accused employee for any clarification to gather additional information
- FIC shall examine the field investigation report and the response by the accused employee (if any) before taking final decision on classification of fraud and penal action if any. The FIC shall be headed by the CRO
- Once the incident is declared/classified as fraud, a reasoned order containing the relevant facts shall be made to the accused
- In cases of fraud involving MD, CEO or any employee of CXO grade, the entire process of investigation and staff accountability shall be handled by the audit committee of the board (ACB). Such executive shall not take part in any meeting in which their accountability is examined.

6.2.4 Reporting of Fraud

- The company shall furnish the fraud report as FMR to RBI within 14 days of FIC making the classification as "fraud". Risk management function shall be responsible for this reporting.
- Incident of fraud shall be reported to the law enforcement agency as soon as the investigation team draws a reasonable suspicion of fraud being committed
- FIR shall be filed for fraud cases. Instances where FIR is not filed due to various obstacle, the reason needs to be documented.
- Fraud cases can be "closed" where the three years has lapsed since filing of FIR and amount involved is less than 25 lakhs provided staff accountability action is completed

6.2.5 Entities / Customers classified as Fraud

- The company shall not extend credit to any person who has been reported / classified as fraud provided such information is available in public domain or can be sourced easily from public entities

7. Information Technology Risk Management:

Company depends on technology-intensive information systems to successfully carry out its

mission and business functions. Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., realizing the mission, daily functioning, image or reputation), organizational assets and individual by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity or availability of the information being processed, stored, or transmitted by the systems.

It is imperative that all users of Company understand their responsibilities and are held accountable for managing information risk – that is, the risk associated with the operation and use of information systems that support the mission and business functions of company I.e. cyber security risk.

i. Sources of Information Risk

IT Risk Management shall work on the following principle.

- **Confidentiality** – Ensuring access to sensitive data to authorized users only.
- **Integrity** – Ensuring the accuracy and reliability of information by ensuring that there is no modification without authorization.
- **Availability** – Ensuring that uninterrupted data is available to users when it is needed.
- **Authenticity** – For IS (information security) it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

ii. IS Policy framework:

The IT policy shall provide for an Information Security framework incorporating following aspects:

- Identification and Classification of Information Assets – Company shall keep a complete inventory of Information Asset with the distinct and clear identification of the asset.
- Segregation of functions – There must be a separation of the duties of the Security Officer/Group and the Information Technology division which actually implements the computer systems. The IS function must be sufficiently resourced in terms of the number of workforces, level of skill & tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc. Further, there should be clear segregation of responsibilities relating to system administration, database administration and transaction processing.
- Role-based Access Control – Access to information should be based on well-defined user roles (system administrator, user manager, application owner, etc.), There should be a clear delegation of authority for the right to upgrade/change user-profiles and permissions and also key business parameters which should be documented.
- Personnel Security – A few authorized application owners/users may have intimate knowledge of financial institution processes and they pose a potential threat to systems and data. CA Grameen should have a process of appropriate check and balance in this regard. Personnel with privileged access to the system administrator, cybersecurity personnel, etc. should be subject to rigorous background check and screening.
- Physical Security – The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. CA Grameen should have a secured environment for the physical security of IS Assets such as the secure location of critical data, restricted access to sensitive areas like data centre.
- Maker-checker is one of the important principles of authorization in the information systems of financial entities. For each transaction, there must be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure the reliability of the information.
- Incident Management – Company shall define what constitutes an "incident". The Company shall develop and implement processes for preventing, detecting, analysing and responding to information security incidents.
- CA Grameen shall ensure that audit trails exist for IT assets satisfying its business requirements including regulatory and legal requirements, facilitating the audit, serving as forensic evidence when required and assisting in dispute resolution. If an employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.
- Cyber Crisis Management Plan (CCMP) must be evolved & must be a part of the overall IT

strategy. CCMP must report the following four aspects: i) Detection ii) Response iii) Recovery and iv) Containment.

- Suitable policy and procedure shall be adopted under that addresses the risk arising out of vendor empanelment, selection and risk of non-performance. This is separately covered in Vendor Risk management policy.
- The company shall take up a comprehensive assessment of IT related risks (both inherent and potential risk) including the cyber security risk and review/update every year. The summary of key identified risks shall be presented to both, Risk Management Committee and IT Strategy Committee.

iii. Roles and Responsibilities of Information Risk Management:

- The detailed governance structure for managing IT/Cyber risk has been laid out in a separate board approved policy – "Information Security Governance Framework".

8. New Product Approval:

As a leading microfinance company in the country, CA Grameen will be adopting new products and product variants depending upon the requirements of customers, from time to time. New product shall be launched with a pilot process with a limit on the exposure.

Respective business unit shall be responsible for designing the new product and preparing the product approval note. This will include identifying the need for new product, defining product characteristics, assessing business opportunity and profitability. They will also design the pilot process including the target segment and geography for the pilot launch, metrics and thresholds for evaluating pilot performance along with the plan for full scale roll-out. Risk function will review the credit risk associated with the product and check against risk appetite. Further, the Risk team will provide insights on market risk, operational risk, and reputational risk related to the new product while the Compliance function will provide guidance on compliance risks to ensure we fully adhere to regulatory requirements. The completed product note shall be presented by the respective business unit to the New Products Committee (NPC).

Roles and Responsibilities with respect to New Product Development:

1. The NPC shall be responsible for evaluating and approving new products and ensuring they align with the organization's strategic objectives and regulatory requirements.
2. Respective Business Head or Head-Product shall prepare a comprehensive product note identifying potential operational, financial, and compliance risks associated with their introduction.
3. The NPC shall ensure adherence with the requirements prescribed under the Compliance Policy and various other applicable RBI Regulations from time to time.
4. The Risk team shall define the credit policy with respect to new product in consultation with other stakeholders; the credit policy shall be part of the product note presented to the NPC
5. Respective Businesses shall prepare a manual detailing the procedure involved in delivery of the product
6. The product note including credit policy shall be approved by the Board upon recommendation from RMC

9. New Branch Approval

To ensure controlled expansion of the organization, CA Grameen shall manage opening of new branches only after comprehensive review of respective business and risk factors in each proposed location.

A consolidated branch survey report for each proposed location consisting of all information with respect to Census, industry exposure, demographics, PAR data, business viability of location etc. shall be shared by the strategy and innovations team with respective business heads. Post review, business heads shall recommend opening of new branches in respective locations.

The risk team may undertake independent geographical risk surveys for proposed location. The survey would provide insight of all inherent risks for building further mitigation.

The completed branch survey report including business heads recommendation and risk survey report shall be shared with the Branch Opening Approval Committee (BOC) consisting of CEO, COO, CRO & CFO. The BOC shall provide approval for the recommended locations.

Roles and Responsibilities with respect to branch expansion:

- Business team shall submit the new branch opening proposal (Branch Opening Survey Report) to BOC. This includes information on demographics, industry exposure and business viability in each location.
- The risk team may perform independent/parallel geographical risk assessment and provide views/mitigants.
- The Branch Opening Approval Committee shall accord the approval after reviewing the proposal.

10. Model Risk Management:

Model Risk is defined as risk of losses relating to the development, implementation, or improper use of models by the institution for decision-making with respect to customer risk assessment, loss forecasting, product pricing, evaluation of hedging instruments etc. CA Grameen may use various quantitative techniques for customer underwriting, loss forecasting, upsell, cross-sell, measurement of interest /currency risk and ECL measurement.

Definition of Model

Model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. For example, an estimate calculated based on simple average or other simple arithmetic & logical operation shall not be considered as model.

CA Grameen shall abide by the following principles while using models for decision making:

- A model inventory must be maintained, and all models must be categorized as critical or non-critical depending on how large the impact is on company's business. A Model which meets any of the below criteria shall be deemed as "critical":
    - The model is used for underwriting >5% of aggregate disbursed loan.
    - The model is used to estimate any component of financial statement to the extent that the component is >5% of total assets or >5% of total revenue.
- All models must be back tested before use. For external models, appropriate data may be

obtained from model providers to satisfy the back-testing requirement.

- All models must be reviewed/validated every two years to ensure that model has maintained its predictive ability.
- Critical models shall require enhanced monitoring. Such models need to be externally validated every 12 months.
- Risk management function shall perform all model validation exercise (except critical models), however, CRO may decide to engage external agency depending on complexity of the model.
- It shall be ensured that staff doing the model validation work has not been involved in the model development process. In addition, the validation result needs to be reviewed by the Chief Risk Officer who may specify remedial action whenever necessary.

Roles and Responsibilities of Model Risk Management:

- The respective departments shall be responsible for development, use and maintenance of the models.
- Risk team (CRO or a designated officer within the Risk department) shall accord the approval for model usage.
- The Risk team shall be responsible for managing the model categorization, model inventory and periodic validation.

11. Climate Change Risk

Climate change risk is defined as loss due to long term pattern change in extreme weather events such as drought, flood, cyclone, earthquake etc. Low-income customers being the primary target segment for CA Grameen; this risk poses added vulnerability to the business model.

CA Grameen shall abide by the following principle while dealing with the climate change risk:

- Extreme weather events within CA Grameen operational geography shall be recorded as risk incident. Resultant loss / disruptions incurred by CA Grameen must also be recorded wherever data is available.
- Company shall undertake periodic assessment of climate change risk taking into account recorded events and forecast (e.g. El Nino, monsoon forecast etc.) available in the public domain. Such assessment will be presented to the MLRC at least annually. The assessment shall include possible impact and suggested control to mitigate such risk.

12. Risk Data Aggregation and Risk Reporting Practices

The risk data aggregation capabilities and risk reporting practices should be fully documented and subject to high standards of validation that are aligned with the company's risk assessment and risk control and self-assessment review.

The validation of risk data aggregation and risk reporting practices shall be conducted using staff with specific data and reporting expertise. Following risk reports shall go through high level of validation before publication: (1) Quarterly Portfolio Trend Report (RMC) (2) Monthly Portfolio Trend Report (MLRC) (3) Quarterly Expected Credit Losses (ECL) Computation. The risk management function shall have a well-documented process for validation to ensure that relevant risk reports are accurate. Adequate resources with relevant skillset and expertise shall be deployed for this purpose.

Further, the risk management function shall ensure that data quality risks are included within the risk control self-assessment (RCSA) process. The assessment should include both outsourced (if

any) and in-house risk data-related processes and aspects such as data confidentiality, integrity and availability.

13. Policy Review

This policy shall be reviewed by the Board of Directors at least on an annual basis or such frequent intervals as may be required, and updated based on the recommendations of the Risk Management Committee of the Board.