CREDITACCESS GRAMEEN LIMITED

Vendor & Outsourcing Management Policy

Version 2.2

Revision History

Version	Author	Description of Changes	Release Date
1.0	Arakapu Jagadeesh	Adoption	March 23, 2022
1.0	Arakapu Jagadeesh	Re-adoption	April 01, 2024
2.0	Saul Ruth S Ambat	Revised to Combine Vendor Management Policy with IT Outsourcing Policy and Financial Outsourcing Guidelines by the RBI	October 25, 2024
2.0	Saul Ruth S Ambat	Re-Adoption	April 21, 2025
2.1	Saul Ruth S Ambat	1. Section 7.3 (iii)- Added clause for collection of SBOM during procurement of any critical application / software 2. Section 7.3 (iv) – Added Minimum elements to be considered in SBOM 3. Section 7.4(iv) – Added clause for review of SBOM by Infosec 4. Section 7.6 (x) – Added SBOM clauses to be considered in a contract 5. Section 7.7(iii) Added clause to consider annual review of SBOM 6. Section 9.i (t) Added collection of SBOM for critical applications as part of vendor onboarding requirements 7. Section 11.i(n) – Added clause for review of SBOM during the annual vendor risk assessment	May 16, 2025
2.2	Shruthi Laxmain	Below Sections are updated as per the New guidelines : Reserve Bank of India (Non-Banking Financial Companies – Managing Risks in Outsourcing) Directions, 2025 dated November 28, 2025 . Section 9: isk Assessment at Onboarding (Updated) Section 11: Periodic Review of Vendor Risk (Updated) Section 12 : Outsourcing - Definition (Updated) Section 12.2 : Authorization, Accountability and Oversight Guidelines (New Section)	May 08, 2026

		Section 12.3: Guidelines for IT Outsourcing (Updated) Section 12.4: Outsourcing of Security Operations Center (SOC) (New Section) Section 12.5: Business Continuity and management of Disaster Recovery Plan (New Section) Section 12.6: Requirements for cloud computing solutions (Updated) Section 12.7: Guidelines for Financial Services Outsourcing (Updated) Section 12.8: Outsourcing within a Group / Conglomerate (Intra -Group Arrangements) (New Section) Section 12.9: Offshore and Cross-Border Outsourcing (New Section) Section 12.10: Pre-Outsourcing Evaluation for Material IT Outsourcing (New Section) Section 13: Roles and Responsibilities (Updated)	

Version Control

Version	Author	Reviewed by	Approved by
1.0	Arakapu Jagadeesh – Asst. Manager (Risk)	Firoz Anam - Chief Risk Officer Sudesh Puthran – Chief Technology Officer	Board of Directors
1.0	Arakapu Jagadeesh – Asst. Manager (Risk)	Firoz Anam - Chief Risk Officer Sudesh Puthran – Chief Technology Officer	Board of Directors
2.0	Saul Ruth S Ambat – Senior Manager -IT GRC	Firoz Anam - Chief Risk Officer Ravi Rathinam - Chief Information Security Officer Sudesh Puthran – Chief Technology Officer	Board of Directors
2.1	Saul Ruth S Ambat – Senior Manager -IT GRC	Firoz Anam - Chief Risk Officer Ravi Rathinam - Chief Information Security Officer Sudesh Puthran – Chief Technology Officer	Board of Directors

2.2	Shruthi Laxmain AGM – IT GRC	Ravi Rathinam - Chief Information Security Officer Firoz Anam - Chief Risk Officer Sudesh Puthran – Chief Technology Officer Recommended By : Ganesh Narayanan MD and CEO	Board of Directors

1. Introduction

CreditAccess Grameen Limited ("CA Grameen" or "the Company") engages third-party service providers and suppliers/vendors to deliver select business functions, leveraging external expertise and cost efficiencies where these cannot be optimally achieved through internal resources alone. Vendor Management is the structured process by which the Company governs its outsourcing arrangements to ensure that the engagement of service providers does not expose the organisation to unacceptable levels of operational risk, business disruption, or adverse impact on service quality, customer outcomes, or regulatory compliance. This Policy establishes the governance framework applicable to all outsourcing activities undertaken by CA Grameen, covering the complete lifecycle of each arrangement — from the initial identification of a business need and vendor selection, through contract execution and performance oversight, to contract renewal or termination.

2. Reference

a. RBI Master Direction – IT Outsourcing
b. RBI Master Direction - Managing Risks and Code of Conduct in Outsourcing Financial Services

3. Abbreviations

Abbreviation	Meaning
IT	Information Technology
IS	Information Systems
CAGL	CreditAccess Grameen Limited
BCP	Business Continuity Plan
DR	Disaster Recovery
RBI	Reserve Bank of India
NBFC	Non-Banking Financial Company
MFI	Micro Finance Institution
CSP	Cloud Service Provider
KMP	Key Managerial Personnel

4. Scope

This Policy establishes the requirements for implementing, maintaining, and continually improving CA Grameen's Vendor Management framework across all outsourced services. It sets out the criteria for assessing the materiality of specific outsourcing activities and the corresponding risk management requirements. The Policy applies to the Board, Senior Management, the Purchase Committee, the Information Security function,

business unit users, and all third-party service providers engaged by CA Grameen, irrespective of their location. It also governs the conduct of suppliers and their personnel, ensuring alignment with CA Grameen's standards on environmental responsibility, human rights, and ethical business practice.

5. Principles of Vendor Risk Management

CA Grameen is committed to the ethical and prudent management of all outsourced services. The Company shall ensure the protection of information belonging to clients, licensees, employees, and all other proprietary information held within CA Grameen's information-processing systems and facilities throughout the duration of any outsourcing arrangement. This Policy reflects the Board's directive on vendor management and shall be communicated to all relevant internal stakeholders and shared with interested parties, as appropriate, following necessary approvals.

The salient principles are as follows:

a. Maintain a fair and transparent procurement system that provides equal opportunity to all eligible third parties.
b. Clearly define and document roles and responsibilities for vendor management across all relevant functions.
c. Ensure that all outsourcing-related risks are identified and assessed prior to vendor onboarding, with continuous monitoring and remediation of risks conducted through periodic assessments.
d. Allocate sufficient resources to establish, implement, operate, monitor, review, maintain, and continually improve the vendor management process.
e. Ensure that all third parties engaged under this Policy are contractually bound to adhere to applicable legal and regulatory requirements through legally enforceable agreements.
f. Ensure that policies, standards, procedures, and guidelines supporting vendor management are developed, periodically reviewed, and updated as required.

6. Vendor's Code of Conduct

6.1. Environment Sustainability

i. Suppliers shall comply with all applicable laws, including those relating to environmental sustainability and protection, while performing any work for CA Grameen.
ii. Suppliers shall establish operational practices that minimise environmental impact and deploy measures to prevent and reduce harm to the environment.
iii. Suppliers shall promote the efficient use of natural resources and apply energy-efficient, environmentally friendly technologies, reducing waste and emissions to air, water, and soil.
iv. Suppliers shall comply with waste segregation and disposal rules prescribed by central, state, and local authorities.

v. Suppliers shall actively work to improve environmental conditions in the communities in which they operate and minimise their impact on biodiversity and climate change.

6.2. Social Responsibility

i. Suppliers shall comply with all applicable employment laws, labour legislation, and human rights standards in every jurisdiction in which they operate.

ii. Suppliers shall commit to eliminating all forms of forced labour, bonded labour, and child labour from their operations and supply chains.

iii. Suppliers shall provide their employees with a workplace free from harsh or inhumane treatment, including sexual harassment, sexual abuse, corporal punishment, torture, mental or physical coercion, and verbal abuse. Threats of any such treatment are equally prohibited.

iv. Suppliers shall provide a safe working environment through proactive management and appropriate controls that minimise health and safety risks and support accident prevention.

v. All employees shall be remunerated at a level commensurate with prevailing industry conditions or the applicable minimum wage, whichever is higher.

vi. Suppliers shall ensure that employees have access to an effective grievance reporting mechanism and that open communication between management and employees is actively facilitated. Suppliers shall be responsible for the timely payment of fair wages.

vii. Suppliers shall maintain a work environment free from discrimination on the grounds of race, colour, age, gender, sexual orientation, ethnic origin, religious beliefs, political views, or any other protected characteristic. Staff recruitment practices shall comply with the principle of equal opportunity.

7. Vendor Management / Governance Process

7.1. Discovering a business need

i. The relevant business function shall determine whether there is a need to improve an existing process, reduce costs, or deliver a new product or service.

ii. Once the need is identified, a cost-benefit analysis shall be undertaken to inform the decision to deploy internal resources or engage an external service provider. Outsourcing is typically considered where an external provider can deliver the service more efficiently, at higher quality, or at lower cost than internal execution.

iii. Any decision to outsource an activity shall be aligned with the long-term strategic interests of CA Grameen and shall not result in an undue increase in the Company's risk profile.

iv. The materiality of any proposed outsourcing activity shall be assessed by the relevant Head of Department prior to initiating a financial or IT outsourcing decision.

v. The materiality of an outsourced activity shall be assessed on a gross basis, considering the following factors:

a. The importance of the outsourced activity to CA Grameen, as measured by the proportion of customers or revenue covered by the activity.
b. The potential impact of the outsourcing arrangement on CA Grameen's solvency, liquidity, capital adequacy, and total operating costs.
c. The potential impact of outsourcing on brand value, reputation, and the ability to achieve business objectives, plans and strategies if the service provider fails to perform.
d. Cost of outsourcing as a proportion of total operating cost of the department.
e. The aggregate concentration risk arising from the use of the same service provider across multiple outsourced activities.
f. The potential impact on customer service levels arising from the outsourcing of the activity.
g. The degree of difficulty, including the time and cost required, to identify an alternative service provider or bring the activity back in-house.
h. The potential impact on financial markets and CA Grameen's counterparties in the event of service provider failure.

vi. Where the overall materiality assessment indicates a high level of risk, the final decision to proceed with the outsourcing arrangement shall require Board approval.

7.2. Developing the scope of work

i. The scope of work shall be defined to align precisely with the business need identified during the requirements assessment stage.

ii. CA Grameen shall maintain a centralised vendor register and, prior to commencing a new vendor engagement, shall review existing vendor relationships to determine whether the requirements can be met by expanding the scope of an existing arrangement.

7.3. Issuing request for proposals (RFP)

i. To ensure the selection of the most suitable vendor, the relevant function shall issue a formal Request for Proposal (RFP) or Request for Information (RFI) for critical and significant vendor categories or outsourcing activities.

ii. Where the vendor is expected to manage a core business process, a cross-functional team shall be constituted to develop and finalise the RFP.

iii. A Software Bill of Materials (SBOM) shall be mandatorily collected during the procurement of any critical software or application. Vendors shall be required to demonstrate their SBOM generation process and provide SBOMs that can be validated for completeness and accuracy, including a clear listing of all dependencies and open-source components.

iv. As a minimum, each SBOM shall contain the following elements:

a. Component Name - The name of the software component, library, or package
b. Component Version - The exact version or release number of the component being used

c. Component Supplier - The organization or individual responsible for creating, maintaining, or distributing the component
d. Dependency Relationship - A clear mapping of how components are related or nested
e. Component Description - A summary explaining the purpose or functionality of the component
f. Licensing Information - Details about the open-source or proprietary licenses that govern the use of the component
g. Hash or Checksum - A cryptographic hash (e.g., SHA-256) to verify the integrity and authenticity of the component.
h. Author/Creator Information - Who developed or authored the component—may include contact details or Git repository links
i. Timestamp - Date and time when the SBOM was created or last updated
j. Vulnerabilities - Known vulnerabilities of the components
k. Patch Status – Patch or update status of the component, indicating whether any patches are available to fix the known vulnerabilities.
l. Release & End of life Date – Release date of the software with the end of life of the software component
m. Criticality – Criticality or importance of the component to the overall functionality and
n. Unique identifier - A unique identifier to help track and match components accurately across systems
o. Executable property – Attributes indicating whether the component within an SBOM can be executed
p. Archive property – Attributes indicating whether the component within an SBOM is stored as an archived or compressed file
q. Structured property – Attributes indicating the organized format of data within a component listed in SBOM

7.4. Conducting due diligence

i. The relevant function shall remain alert to heightened risk exposure across strategic, reputational, compliance, operational, transactional, social media, and credit risk areas. Additional guidance on due diligence requirements is set out in the sections that follow.
ii. Attention shall be given to assessing how the vendor handles sensitive customer information and whether its practices satisfy applicable regulatory requirements.
iii. The vendor shall disclose any direct or indirect interest held by any employee or director of CA Grameen in the vendor entity.
iv. The SBOM obtained from vendors shall be reviewed and approved by the Information Security function to identify and assess any security vulnerabilities or gaps.

7.5. Selection of Vendor

i. The relevant Head of Department shall evaluate all proposals received and select the vendor best suited to deliver the proposed scope of work.

ii. Vendor evaluation shall be conducted against objective, pre-defined criteria to the greatest extent practicable.

iii. The Head of Department shall obtain the necessary approvals in accordance with CA Grameen's expenditure approval framework.

7.6. Negotiating contracts for critical / significant vendors

i. The relevant function shall ensure that all contracts incorporate appropriate information security clauses. The Information Security function shall be consulted and may provide support in this regard.

ii. All contracts with outsourcing partners shall include CA Grameen's right to audit the vendor and its subcontractors.

iii. The contract shall require the vendor to notify CA Grameen promptly upon the occurrence of any material event, including financial difficulty, catastrophic events, information security incidents, significant changes in strategic direction, or substantial changes in key personnel.

iv. Contracts shall include precise, measurable performance parameters and a clearly defined scope of work, establishing unambiguous expectations with respect to vendor responsibilities.

v. The contract shall specify the consequences of performance failures and, where applicable, any incentives for superior performance. A clearly defined exit clause shall be included in all contracts.

vi. Background verification checks shall be conducted on relevant vendor personnel, and non-disclosure and security policy compliance agreements shall be executed prior to commencement of services.

vii. Contracts shall include clauses governing audit trails, record retention, and the provision of evidence to CA Grameen upon request.

viii. Contracts shall clearly specify payment terms, escalation procedures, and complaint-handling mechanisms.

ix. All Outsourcing agreements should have the minimum set of legal clauses as specified by RBI master directions

x. All contracts with any critical software or application service provider should contain clauses for the creation, update and periodic review of SBOM. Contracts should also include clauses for non-compliance, including applicable penalties for failure to provide the required SBOM

7.7. Monitoring Performance

i. The relevant function shall periodically monitor vendor performance and assess associated risks in accordance with Section 11 of this Policy.

ii. Regardless of which business unit manages the day-to-day vendor relationship, all key vendor information shall be maintained in the centralised vendor register in accordance with Section 10 of this Policy.

iii. The relevant function shall develop and maintain key performance indicators (KPIs) to monitor vendor performance where practicable. KPIs shall be reviewed at each periodic assessment. For critical software or application vendors, the annual review shall also include a review of the SBOM.

iv. Any change to services provided by a vendor shall be subject to thorough review, including an assessment of information security implications, prior to agreement, to ensure that the effectiveness of existing controls is maintained.

7.8. Terminating or Renewing Contracts

i. The relevant function shall review the business case for each vendor engagement prior to contract renewal, determining whether to continue outsourcing or develop an in-house capability.

ii. Taking into account the vendor's performance and prevailing market conditions, CA Grameen shall assess whether it is more advantageous to renew the existing arrangement or establish a new vendor relationship, ensuring continuity of service throughout any transition.

iii. The relevant function shall maintain a contingency plan to manage service continuity in the event that the vendor becomes unreliable or the relationship requires termination.

iv. Upon termination of a vendor contract, the relevant function shall ensure that all contract documentation is archived and retained in accordance with applicable regulatory and legal requirements.

8. Vendor Categorization

Vendors shall be classified into three tiers based on their criticality to CA Grameen's operations:

i. Critical – A vendor is classified as Critical if its failure to deliver services as contracted, or a breach of its systems, has the potential to cause significant financial loss, business disruption exceeding 24 hours, reputational damage, or regulatory non-compliance. Examples include data centre operators and core application vendors.

- **Any activity which is classified as Material IT outsourcing(Section 12.3) or Material Financial outsourcing , the vendor performing this activity shall necessarily be classified as critical**.

ii. Significant – A vendor is classified as Significant if it provides services that support CA Grameen's operational efficiency. The impact of its failure is limited to financial loss from reduced efficiency or business disruption of less than 24 hours. Examples include internet service providers.

iii. Non-Essential – A vendor is classified as Non-Essential if an alternative can be

readily sourced with minimal disruption to service levels or customer experience. Examples include office supplies.

9. Risk Assessment at Onboarding

i. Prior to finalising vendor selection, appropriate due diligence shall be conducted on each shortlisted vendor. The depth of due diligence shall be proportionate to the criticality of the vendor relationship and shall cover the following areas:
   a. Qualitative, quantitative, financial, operational, legal, and reputational factors
   b. Corporate existence, business history, and market standing, including the vendor's track record and market share in the relevant service area.
   c. Financial strength and solvency, including the vendor's ability to sustain delivery of the contracted services.
   d. Key-person dependency, including whether the departure of one or two individuals could materially impair service delivery.
   e. Qualifications, backgrounds, and reputations of the vendor's principals, including criminal background checks where appropriate.
   f. Vendor's reputation (including adverse media reports) and past performance with similar business partners.
   g. The vendor's experience and competence to implement, support, and sustain the outsourced activity throughout the contracted period, and its ability to serve all customers with the required level of confidentiality (mandatory for financial outsourcing arrangements).
   h. Internal control environment: CA Grameen shall review the vendor's audit reports, internal control evaluations, and third-party assessments, as applicable.
   i. **Contractual & Legal risk** including but not limited to any legal precedents/fines enforced/ penalties paid/ private settlements made and strength of such cases to understand potential litigations and ease of enforcing the contract. (Primarily for financial outsourcing)
   j. Compliance risk: This shall include a review of any regulatory enforcement actions and anti-bribery or corruption risk.
   k. The vendor's reliance on, and demonstrated success in managing, third-party sub-service providers.
   l. The nature and extent of access the vendor will have to CA Grameen's information assets, and the sensitivity and value of the information involved.Ability to comply with information security requirements, including data protection, data privacy and data retention requirements as per regulations.
   m. Ability to meet disaster recovery and business continuity requirements.
   n. Whether any employee or director of CA Grameen holds a direct or indirect interest in the vendor.
   o. **Concentration of risk** arising from using the same service provider for

multiple outsourced activities and using the same service provider used across industry for same outsourced activities.

p. Ensure that the vendor has necessary insurance coverage
q. **Country Risk** – due to the political, social or legal climate creating added risk
r. **Jurisdictional risk**– due to the political, social or legal climate of the service providers jurisdiction creating added risk
s. **Exit strategy risk** - ease of moving the services from one vendor to another or back in house (Applicable primarily for outsourced vendors)
t. Whether the vendor has a detailed SBOM in place with all the minimum set of components as described in this policy. (Only for Critical application / software service providers)
u. Financial soundness and ability to service commitments even under adverse conditions;
v. Security and internal control, audit coverage, reporting, and monitoring procedures, and business continuity management; and
w. External factors like political, economic, social, and legal environment of the jurisdiction in which the service provider operates and other events that may impact data security and service performance.
x. Where possible, an CA Grameen shall obtain independent reviews and market feedback on the service provider to supplement the findings of its own due diligence.
y. CA Grameen shall also evaluate whether the systems of its service provider are compatible with those of CA Grameen, and the acceptability of their standards of performance including in the area of customer service
z. Outsourcing of IT services, with the following additional considerations:
    - technology, infrastructural stability, data backup arrangements, and disaster recovery plan;
    - conflict of interest, if any;
    - capability to identify, and segregate CAGrameen's data;
    - capability to comply with the regulatory and legal requirements of the outsourcing arrangement;
    - information / cyber security risk assessment;
    - ensuring that appropriate controls, assurance requirements, and possible contractual arrangements are in place to ensure data protection and CA Grameen's access to the data which is processed, managed or stored by the service provider;
    - ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities; and
    - ability to enforce agreements and the rights available thereunder including those relating to aspects such as data storage, data protection, and confidentiality.

ii. The Risk Management function shall maintain a detailed due diligence checklist

covering all applicable risk areas, which shall be shared with the relevant Heads of Department and vendor managers at the time of onboarding.

iii. The scope and depth of due diligence shall be calibrated to the vendor's classification, in accordance with the matrix set out below:

Parameter	Critical	Significant	Non-Significant
Corporate History	Y	Y	-
Financial Strength	Y	Y	-
Employee Profile	Y	Y	-
Internal Control	Y	Y	-
DR/ BCP	Y	-	-
Information Security	Y	Y	-
Data Protection	Y	Y	Y , if relevant
Third Party Reliance	Y	-	-
Reputation	Y	Y	Y
Insurance Coverage	Y	-	-
Anti-Bribery / Corruption	Y	Y	Y
Country Risk	Y	Y	Y

10. Vendor Inventory

i. CA Grameen shall maintain a centralised vendor register comprising, at a minimum, each vendor's name, description of services provided, criticality classification, date of last review, and relationship owner. The register shall be kept current at all times.

ii. A centralised inventory of all IT and financial services outsourced to third-party providers, including key entities in their supply chains, shall also be maintained.

11. Periodic Review of Vendor Risk

i. Periodic reviews of vendor risk shall be conducted by the relevant vendor relationship owner. At a minimum, each review shall assess the following:

   a. Counterparty Risk: Whether the vendor has performed in accordance with contractual expectations since the last review, or whether any material deficiencies have been identified.

   b. , owing to outsourcing, the privacy, consumer, and prudential laws are not adequately complied with.Compliance Risk: Whether, owing to the outsourcing arrangement, applicable privacy, consumer protection, or prudential laws have been inadequately complied with.

   c. Contractual Risk: Whether any breach of contract, regulatory non-compliance, or enforcement action has occurred, and whether CA Grameen retains the ability to enforce its contractual rights against the service provider.

   / regulatory requirements and actions taken against the vendor. where the

CA Grameen may not have the ability to enforce the contract with the service provider.

d. Jurisdictional and Country Risk: The current political, social, or legal climate in the service provider's jurisdiction or country of operation.
e. Exit Strategy: Whether a documented exit strategy is in place and whether CA Grameen has reviewed any over-reliance on a single vendor across multiple services. (Applicable to Critical vendors only.)
f. Strategic Risk: Whether the vendor's service delivery remains consistent with CA Grameen's overall strategic direction. (Applicable to financial outsourcing only.)
g. Whether there has been a material deterioration in the vendor's financial position since the last review.
h. Whether there have been changes in senior management or the loss of key personnel that may adversely affect service delivery.
i. Whether any cyber security incidents have occurred at the vendor's premises, and any relevant observations from IT audit reports.
j. Whether any adverse media coverage (print or social media) has emerged that could affect service delivery or pose a reputational risk to CA Grameen.
k. Whether the relevant function has a contingency plan in place to manage disruptions at the vendor's end. (Applicable to Critical vendors only.)
l. Whether any CA Grameen employee or director holds a direct or indirect interest in the vendor.
m. Operational Risk: Any operational continuity risk arising from the use of outdated technology, inadequate processes, or any frauds or errors identified during the review period. (Primarily applicable to financial outsourcing.)
n. Reputational Risk: Whether the standard of service delivery and customer interaction by the service provider meets CA Grameen's requirements and whether confidentiality obligations are being upheld. (Applicable to financial outsourcing only.)
o. Whether a detailed and current SBOM is maintained for each critical software or application vendor.
p. Legal Risk – where CA Grameen is subjected to, fines, penalties, or punitive damages resulting from supervisory actions, or private settlements due to omissions and commissions by the service provider. (Only for financial outsourcing)
q. Exit Strategy Risk – may arise when an CA Grameen becomes over reliant on one service provider, loses relevant internal skills preventing it from bringing the activity back in-house, or enters into contracts that make speedy exits prohibitively expensive. (Only for financial outsourcing)
r. Counterparty Risk – such as where the service provider engages in inappropriate underwriting or credit assessments. (Only for financial outsourcing)

s. Country Risk – where the political, social, or legal climate creates added risk in the outsourcing arrangement. (Only for financial outsourcing)
t. Concentration and Systemic Risk – where there is a lack of control of an CA Grameen over a service provider, more so when overall industry has considerable exposure to one service provider. (Only for financial outsourcing)

ii. The Risk Management function shall maintain a detailed periodic review checklist covering all applicable risk areas. This shall be shared with the relevant Heads of Department and vendor owners as and when required.

iii. Frequency of Periodic Reviews
a. All outsourced service providers shall be treated as Critical vendors for the purpose of scheduling reviews. A half-yearly review of all material financial outsourcing arrangements shall be conducted in addition to the periodic risk assessments set out in the table below.

Vendor Criticality	Risk Level	Risk Monitoring frequency
Critical	High	At least once per year
Significant	Medium	Every other year
Non-essential	Low	Not Required

12. Outsourcing - Definition

For the purposes of this Policy, "outsourcing" means CA Grameen's use of a third party — whether an affiliated entity within the corporate group or an external entity — to perform activities on a continuing basis that would normally be undertaken by CA Grameen itself, currently or in the future. 'Continuing basis' includes arrangements for a defined, limited period.

This section addresses two categories of outsourcing:

i. IT Services Outsourcing
Outsourcing of IT services shall include outsourcing of the following IT Activities:
a. IT infrastructure management, maintenance and support (hardware, software or firmware)
b. Network and security solutions, maintenance (hardware, software or firmware)
c. Application Development, Maintenance and Testing; Application Service Providers (ASPs) including ATM Switch ASPs
d. Services and operations related to Data Centers
e. Cloud Computing Services
f. Managed Security Services
g. Management of IT infrastructure and technology services associated with payment system ecosystem

ii. Financial Services Outsourcing

Outsourcing of Financial services shall include outsourcing of the following activities:

a. Application sourcing (e.g., customer sourcing through DSA))
b. Middle and back-office operations (e.g., electronic funds transfer, payroll processing, custody operations, quality control, order processing)
c. Claims administration (e.g., loan negotiation, loan processing, collateral management, collection of bad loans) Services and operations related to Data Centers
d. Document processing (e.g., cheques, credit card and bill payments, bank statements, other corporate payments, customer statement printing)
e. Cash management
f. Manpower management (e.g., training and development)
g. Marketing and research (e.g., product development, data warehousing and mining, media relation, call centre, telemarketing)
h. Collection / Debt recovery
i. Legal & technical assessment of collateral

12.1. Activities that Shall not be outsourced

In accordance with RBI Regulations, the following activities shall not be outsourced:

i. Core management functions, including policy formulation and material decision-making processes such as determining compliance with Know Your Customer (KYC) norms.
ii. Loan Sanctioning
    a. The final decision to extend credit shall be made internally by CA Grameen and shall not be delegated to an outsourced service provider.
    b. Even where a Board-approved loan sanctioning template is in use, CA Grameen shall be able to demonstrate that the credit decision was made solely by its internal personnel, with the service provider acting only in a facilitative capacity.
iii. Management of investment portfolio
iv. Compliance Function
v. Internal Audit Function
    a. **Exception:** Experts, including former employees, may be hired on a contractual basis if necessary. The Audit Committee of the Board (ACB) or the Board must be assured that the required expertise is not available within the internal audit function prior to hiring.
    b. Any potential conflict of interest in hiring external experts shall be recognized and effectively addressed.
    c. Ownership of all audit reports shall rest with the regular functionaries of the internal audit function, even when external experts are involved

12.2. Authorization, Accountability and Oversight

CA Grameen shall ensure that

i. All applicable laws, regulations, guidelines, and conditions of approval, licensing, or registration have been duly considered when conducting due diligence in connection with any outsourcing arrangement.

ii. Outsourcing, whether the service provider is located within or outside India, does not impede or interfere with CA Grameen's ability to effectively oversee and manage its activities and fulfil its obligations.

iii. Outsourcing, whether the service provider is in India or outside, does not impede or interfere with the ability of an CA Grameen to effectively oversee and manage its activities, and fulfil its obligations

iv. Outsourcing shall not result in any compromise or weakening of CA Grameen's internal controls, business conduct, or reputation.

v. The service provider employs the same high standard of care in performing the services as would be employed by CA Grameen, if the activities were conducted within CA Grameen and not outsourced; and

vi. The service provider, if not a group company of CA Grameen, shall not be owned or controlled by any director of CA Grameen, or their relatives having the same meaning as assigned under Companies Act, 2013 and the Rules framed thereunder, as amended from time to time.

12.3. Guidelines for IT Outsourcing

Material Outsourcing of IT Services are those which:

- If disrupted or compromised, shall have the potential to significantly impact CA Grameen business operations; or

- May have material impact on CA Grameen customers in the event of any unauthorised access, loss, or theft of customer information;

The following additional controls shall apply to all activities classified as Material Financial Outsourcing as defined in this Policy, in addition to the general vendor management requirements set out above:

i. CA Grameen shall ensure that the service provider implements appropriate safeguards to prevent the commingling of assets, documents, information, and records where a service provider serves multiple financial institutions.

ii. CA Grameen shall ensure that the service provider, if not the group company, shall not be owned/ controlled by any of its directors, KMPs (Key Managerial Personnel) or approver of outsourcing arrangements of CA Grameen or their relatives. Provided that an exception to the above requirement may be made with the approval of Board or a Committee of the Board, followed by appropriate disclosure,

oversight and monitoring of such arrangements.

iii. A risk assessment shall be conducted prior to initiating any financial outsourcing arrangement, and identified risks shall be monitored on an ongoing basis in accordance with Sections 8, 9, 10, and 11 of this Policy. CA Grameen shall also assess and manage the risk of excessive concentration with a single service provider.

iv. Mitigation measures shall be developed and maintained to address events that could lead to business disruption, customer data leakage, or backup failures.

v. When entering into or renewing any IT outsourcing arrangement, appropriate due diligence shall be conducted to assess the service provider's ongoing capability to comply with its obligations under the outsourcing agreement.

vi. All IT outsourcing contracts will include at minimum the following.

1. Requirements to be met/provided by the outsourced service providers.
2. Clear definition of services.
3. Scope of services to be provided.
4. Qualification requirements for personnel including but not limited to training and, competency requirements.
5. Screening requirements for outsourced service provider personnel.
6. Roles and responsibilities
7. Performance requirements or SLA's, formalizing performance criteria to measure the quality and quantity of service levels.
8. Communication processes.
9. Resilience, recovery, and contingency arrangements including business continuity requirements.
10. Definition of changes and process for managing changes.
11. Payment terms including criteria for service credits.
12. Clear allocation of responsibility for regulatory compliance by the outsourced service providers including but not limited to data protection, intellectual property, copyright protection (including licensing) and any other applicable requirements.
13. Retention of requisite audit trails and logs for administrative activities carried out by the outsourced service providers as applicable.
14. Periodic reviews with vendors against the agreement/contract.
15. Definition of complaints and process for complaint management.
16. Processes for escalation management.
17. Process for dispute management.
18. Process for incident reporting and subsequent action including corrective actions.
19. Shall ensure that cyber incidents are reported to the CA Grameen by service provider without undue delay, so that the incident is reported by CA Grameen to the RBI within 6 hours of detection by the service provider
20. Right to audit clauses allowing audit by CA Grameen directly, their appointed auditors, statutory and regulatory auditors such as those from RBI. Right of RBI or person(s) authorized by it to perform inspection of the

service provider and any of its sub-contractors and access CA Grameen IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and its sub-contractors, in relation and as applicable to the scope of the outsourcing arrangement.

21. Right to access necessary records and evidence as necessary based on approved requests.
22. Record retention and evidencing.
23. Non-disclosure agreements clause requiring with respect to information retained by the service provider./confidentiality agreements.
24. Clearly defined exit clauses. termination rights of CA Grameen including the ability to orderly transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable.
25. Risk of unexpected termination of the outsourcing contract / agreement or liquidation of outsourced service providers.
26. Type of material adverse events (e.g., data breaches, denial of service, and service unavailability, relevant to the outsourced service) and the incidents required to be reported to CA Grameen to enable CA Grameen to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.
27. Liability for damages on security breach or leakage of customer data.
28. Access by CA Grameen to all data, books, records, information logs, alerts and business premises relevant to the outsourced service, available with the service provider.
29. Compliance with the provisions of Information Technology Act, 2000, and other applicable legal requirements and standards to protect the customer data
30. Storage of data only in India (as applicable) as per extant regulatory requirements
31. Obligation of the service provider to comply with directions issued by the RBI in relation to the services outsourced to the service provider, through specific contractual terms and conditions specified by the CA Grameen
32. Obligation of the service provider to co-operate with the relevant authorities in case of insolvency or resolution of CA Grameen
33. Provision to consider skilled resources of service providers who provide core services as 'essential personnel' so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on site during exigencies (including pandemic situations)
34. Clause requiring suitable back-to-back arrangements between service providers and the OEMs.CA Grameen shall ensure that outsourcing agreements have necessary clauses on safe removal or destruction of data, hardware and all records (digital and physical), as applicable. The outsourcing agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering, or changing any data during the transition period, unless specifically advised by the regulator or CA

Grameen.

35. A service provider shall be legally obliged to cooperate fully with both the CA Grameen and its new service provider(s) to ensure there is a smooth transition.

vii. CA Grameen shall ensure that data flows between CA Grameen and each outsourced service provider are clearly documented, with responsibilities for each flow unambiguously defined.

viii. A designated single point of contact shall be assigned for each outsourced service provider to facilitate effective relationship management.

ix. Outsourced service providers shall be contractually required to cascade applicable requirements and obligations to entities within their own supply chains.

x. Monitoring and control of outsourced activities:Monitoring and Control of Outsourced Activities

a. CA Grameen shall maintain a management structure for the ongoing monitoring and control of outsourced services. This shall encompass, at a minimum, monitoring of service provider performance, system and resource uptime, service availability, adherence to SLA requirements, and the effectiveness of the incident response mechanism.

b. CA Grameen shall conduct regular audits of service providers (including sub-contractors) with regard to the service outsourced by it. Such audits may be conducted either by CA Grameen internal or external auditors appointed to act on CA Grameen's behalf.

c. The audits shall assess, the performance of the service provider, adequacy of the risk management practices adopted by the service provider, and compliance with laws and regulations. The frequency of the audit shall be determined based on the nature and extent of risk and impact on the CA Grameen from the outsourcing arrangements. Reports on the monitoring and control activities shall be reviewed periodically by the Senior Management, and in case of any adverse development, the same shall be put up to the Board for information.

d. CA Grameen may, subject to its risk assessment, place reliance on globally recognised third-party certifications provided by the service provider in lieu of conducting independent audits.

xi. CA Grameen shall periodically review the financial and operational condition of each service provider to assess its continued ability to meet its contractual obligations. Such reviews shall identify any deterioration or breach in performance standards, confidentiality, security, or operational resilience preparedness.CA Grameen shall ensure that appropriate corrective actions are promptly initiated in response to any violations or deviations identified in relation to outsourced activities.

xii. Outsourced service providers shall be responsible to appropriately communicate requirements applicable to them down their supply chain.

xiii. CA Grameen shall ensure an independent review and audit on a periodic basis for compliance with the legislations, regulations, Board-approved policy, and performance standards and reporting the same to Board/ Board Committee.

xiv. An exit strategy shall be documented and approved by the relevant function head for each material IT outsourcing arrangement.

12.4. Outsourcing of Security Operations Center (SOC)

Centre (SOC) operations by CA Grameen such as data being stored and processed at an external location and managed by the service provider (or its subcontractors) to which the CA Grameen has lesser visibility, CA Grameen, to mitigate the risks, shall adopt the following requirements:Given the heightened risks associated with the outsourcing of Security Operations Centre (SOC) operations — including the storage and processing of data at an external location managed by the service provider or its subcontractors, with reduced direct visibility for CA Grameen — the following additional requirements shall apply to any SOC outsourcing arrangement:

I. Unambiguously identify the owner of assets used in providing the services (e.g., systems, software, source code, processes, and concepts);

II. Ensure that CA Grameen has adequate oversight and ownership over the rule definition, customization and related data / logs, meta-data and analytics (specific to CA Grameen);

III. Assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored or processed periodically.

IV. Integrate the outsourced SOC reporting and escalation process with CA Grameen incident response process.

V. Review the process of handling of the alerts or events.

12.5. Business Continuity and management of Disaster Recovery Plan

I. CA Grameen shall require its service provider to develop and establish a robust framework for documenting, maintaining, and testing business continuity and recovery procedures. CA Grameen shall ensure that the service provider periodically tests the Business Continuity and Recovery Plan and may also consider occasional joint testing and recovery exercises with its service provider.

II. In establishing a viable contingency plan, CA Grameen shall consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, time, and resources that would be involved.

III. CA Grameen shall ensure that its service providers are able to isolate the CA Grameen's information, documents, and records, and other assets so that in

adverse conditions or termination of the agreement, all documents, records of transactions and information given to the service provider, and assets of the CA Grameen, can be removed from the possession of the service provider (in order to continue its business operations); or deleted, destroyed or rendered unusable.

IV. In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency or liquidation of its service provider, CA Grameen shall retain an appropriate level of control over its outsourcing arrangement along with the right to intervene/exit with appropriate measures to continue its business operations without incurring prohibitive expenses and disruption in the operations of the CA Grameen and its services to the customers.

12.6. Requirements for cloud computing solutions and SaaS services

In addition to the general IT outsourcing controls set out above, CA Grameen shall satisfy the following requirements in connection with the storage, processing, and movement of data in cloud environments:

Several cloud deployment and service models have emerged over time. These are generally based on the extent of technology stack that is proposed to be adopted by the consuming entity.

(1) Example - 1:

(i) Some cloud services are:

(a) Infrastructure as a Service (IaaS): The service provides computing, storage, network, and other basic resources so that the client can develop and deploy their applications.

(b) Platform as a Service (PaaS): The service provides software for building application, middleware, database, development environment, and other tools along with the infrastructure to the client.

(c) Software as a Service (SaaS): Client uses the application(s) provided by the service provider on a cloud infrastructure.

(ii) Besides the three common application services, Cloud Service Providers (CSPs) also provide a range of services, viz., Database as a Service, Security as a Service, Storage as a Service, and others with varying risk levels.

(2) Example - 2: Some of the popular deployment models for delivery of cloud services are Private Cloud, Public Cloud, Hybrid Cloud, and Community Cloud.

i. Prior to adopting any cloud solution, CA Grameen shall analyse its business strategy and goals in the context of its existing IT applications and associated costs. Cloud adoption may range from migrating non-business-critical workloads to the cloud, to deploying critical business applications on a SaaS basis, and the appropriate extent of adoption shall be determined through a thorough business technology risk assessment.

ii. Undertake a comprehensive assessment of CA Grameen's business strategy and goals adopted to the existing IT applications' footprint and associated costs. Such assessment shall include, but not be limited to, an analysis of various heads of cloud-related expenditure, such as application refactoring, integration, consulting, migration, and projected recurring expenditure depending on the nature of workloads. The extent of cloud adoption may vary, ranging from migration of non-business critical workloads to the cloud, to deployment of critical business applications such as SaaS, or other combinations in between, and shall be determined based on a duly conducted business technology risk assessment;

iii. CA Grameen shall ensure that its IT outsourcing policy addresses the entire data lifecycle — from data generation, through entry into the cloud environment, to permanent erasure or deletion. All specified procedures shall be consistent with business needs and applicable legal and regulatory requirements.

iv. In adopting cloud services, CA Grameen shall take into account cloud-specific risk factors, including multi-tenancy and multi-location data storage and processing, and shall establish an appropriate risk management framework accordingly. Cloud security is a shared responsibility between CA Grameen and the Cloud Service Provider (CSP).

v. Cloud Governance: CA Grameen shall adopt and demonstrate a well-established and documented cloud adoption policy. Such a policy should, inter alia, identify the activities that can be moved to the cloud, enable and support protection of various stakeholder interests, ensure compliance with regulatory requirements, including those on privacy, security, data sovereignty, recoverability, and data storage requirements, aligned with data classification. The policy should provide for appropriate due diligence to manage and continually monitor the risks associated with CSPs.

vi. CA Grameen shall ensure that the selection of the CSP is based on a comprehensive risk assessment of the CSP. CA Grameen shall enter into a contract only with CSPs subject to jurisdictions that uphold enforceability of agreements and the rights available thereunder to CA Grameen, including those relating to aspects such as data storage, data protection and confidentiality.

vii. Disaster Recovery & Cyber Resilience: CA Grameen business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the CA Grameen can continue its critical operations with minimal disruption of services while ensuring integrity and security.Service and Technology Architecture: ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognized architecture principles and standards. The technology architecture shall

    a. Provide for a standard set of tools and processes to manage containers, images and releases.

    b. Provide for a secure container-based data management, where encryption keys and Hardware Security Modules are under the control of

the CA Grameen.

c. Be protected against data integrity and confidentiality risks, and against co-mingling of data, in case of multi-tenancy environments; and

d. Be resilient and enable smooth recovery in case of failure of any one or combination of components across the cloud architecture with minimal impact on data / information security;

viii. Identity and Access Management (IAM): IAM shall be agreed upon with the CSP and ensured for providing role-based access to the cloud hosted applications, in respect of user-access and privileged-access. Stringent access controls, as applicable for an on-premise application, may be established for identity and access management to cloud-based applications. Segregation of duties and role conflict matrix should be implemented for all kinds of user-access and privileged-access roles in the cloud-hosted application irrespective of the cloud service model. Access provisioning should be governed by principles of 'need to know' and 'least privileges'. In addition, multi-factor authentication should be implemented for access to cloud applications.

ix. Security Controls: CA Grameen shall ensure that the implementation of security controls in the cloud-based application achieves similar or higher degree of control objectives than those achieved in/ by an on-premise applicationSecurity Controls: CA Grameen shall ensure that the security controls implemented for cloud-based applications achieve an equivalent or higher degree of control effectiveness than those applicable to on-premises applications. This includes ensuring secure connectivity through appropriate deployment of network security resources and configurations, appropriate and secure cloud asset configurations, and defined procedures for authorising changes to cloud applications and related resources.

x. Robust Monitoring and Surveillance: CA Grameen shall define minimum monitoring requirements for the cloud environment and shall assess the CSP's information and cyber security capabilities to ensure that the CSP:

a. Maintains an information security policy framework commensurate with its exposures to vulnerabilities and threats

b. Is able to maintain its information / cyber security capability with respect to changes in vulnerabilities and threats, including those resulting from changes to information assets, or its business environment.

c. Has set the nature and frequency of testing of controls in respect of the outsourced services commensurate with the materiality of the services being outsourced by the CA Grameen and the threat environment; and

d. Has mechanisms in place to assess the subcontractors with regards to confidentiality, integrity and availability of the data being shared with them, where applicable.

xi. Appropriate integration of logs, events from the CSP into the CA Grameen SOC, wherever applicable and/ or retention of relevant logs in cloud shall be ensured for incident reporting and handling of incidents relating to services deployed on the cloud.

xii. Ensure that the cyber resilience controls of the CSP complement the CA Grameen's own application security measures, and that both the CA Grameen and the CSP maintain continuous and regular updates of security-related software, including upgrades, fixes, patches, and service packs, to safeguard applications against advanced threats and malware;

xiii. Vulnerability Management: CA Grameen shall ensure that CSPs have a well-governed and structured approach to manage threats and vulnerabilities supported by requisite industry-specific threat intelligence capabilities.

xiv. Disaster Recovery & Cyber Resilience: CA Grameen business continuity framework shall ensure that, in the event of a disaster affecting its cloud services or failure of the CSP, the CA Grameen can continue its critical operations with minimal disruption of services while ensuring integrity and security.

xv. Ensure that the CSP has put in place demonstrative capabilities for preparedness and readiness for cyber resilience as regards cloud services in use by them through, inter alia, robust incident response and recovery practices including conduct of DR drills at various levels of cloud services including necessary stakeholders.

xvi. Develop an exit strategy that shall

   a. Factor, inter alia, agreed processes and turnaround times for returning CA Grameen's service collaterals and data held by the CSP; data completeness and portability; secure purge of CA Grameen's information from the CSP's environment; smooth transition of services; and unambiguous definition of liabilities, damages, penalties and indemnities, which should also be a part of the service level stipulations in SLA;

   b. Include exit plans which align with the ongoing design of applications and service delivery technology stack;

   c. Include contractually agreed exit / termination plans, which specify how the cloud-hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of CA Grameen's business, while maintaining integrity and security; and

   d. Include clauses providing for the prompt and systematic retrieval of all transaction records, customer and operational information, and configuration data from the CSP upon exit or termination, followed by verified purging of CA Grameen's information from the CSP's environment.

xvii. Ensure that the audit / periodic review / third-party certifications cover, as per applicability and cloud usage, inter alia, aspects such as roles and responsibilities

of both CA Grameen and CSP in cloud governance, access and network controls, configurations, monitoring mechanism, data encryption, log review, change management, incident response, and resilience preparedness and testing.

12.7. Guidelines for Financial Services Outsourcing

'Material Outsourcing' means arrangements, which if disrupted, have the potential to significantly impact the business operations, reputation or profitability or customer service. 'Materiality' of outsourcing shall be based on the:

i. Level of importance to CA Grameen of the activity being outsourced as well as the significance of the risk posed by the same;
ii. Potential impact of the outsourcing on CA Grameen on various parameters such as earnings, solvency, liquidity, funding, capital, and risk profile;
iii. Likely impact on CA Grameen reputation and brand value, and ability to achieve its business objectives, strategy, and plans, should the service provider fail to perform the service;
iv. The cost of the outsourcing arrangement as a proportion of the relevant department's total operating costs.
v. Aggregate exposure to that particular service provider, in cases where CA Grameen outsources various functions to the same service provider; and
vi. Significance of activities outsourced in the context of customer service and protection.

In addition to the guidelines prescribed above for Vendor management, the following controls will also be applicable additionally if the activity is categorized as Material financial outsourcing as per the definition given in the policy

vii. CA Grameen shall adhere to all relevant financial laws, regulations, rules, guidelines, and conditions of approval, licensing, or registration when conducting due diligence for financial outsourcing.
viii. CA Grameen shall ensure that the service provider maintains the same high standard of care in financial operations as would be expected if conducted internally Financial outsourcing arrangements shall not compromise or weaken CA Grameen's internal control, business conduct, or reputation
ix. CA Grameen shall ensure the confidentiality of customer financial information with the service provider and retain ultimate control over the outsourced financial activities. All data shared with the service provider will be through secure, encrypted channels and there will be a process in place for secure disposal of data when needed.
x. CA Grameen shall ensure that service provider staff's access to customer information is strictly to what is necessary for performing the outsourced function.
xi. CA Grameen shall ensure that the service provider Implement safeguards to prevent

the comingling of assets, documents, information, and records when a service provider works with multiple financial institution

xii. CA Grameen shall ensure that financial service providers do not impede its ability to effectively oversee and manage financial activities. Service providers must not obstruct the supervisory authority in performing its supervisory functions and achieving its objectives.

xiii. The financial service provider, if not a group company, must not be owned or controlled by any director, key managerial personnel, or approver of the outsourcing arrangement at CA Grameen, or their relatives. Any exceptions to this rule must be approved by the Board or a Committee of the Board and accompanied by appropriate disclosure

xiv. Outsourcing of financial services shall not affect customer rights, including their ability to seek redressal under relevant financial laws

xv. Where agents are engaged for sales, marketing, or other customer-facing activities, CA Grameen shall clearly state in the relevant product literature and brochures that the services of such agents may be utilised, and shall describe the scope of the agents' role in broad terms.

xvi. Risk assessment will be carried out prior to initiating outsourcing and identified risks shall be monitored on an ongoing basis in line with Section 8,9, 10 & 11. The company shall also evaluate the risk of excessive reliance on a single service provider.

xvii. All Financial outsourcing contracts will include at minimum the following. All financial outsourcing agreements shall be vetted by CA Grameen's legal counsel for legal effect and enforceability. Each agreement shall also state the nature of the legal relationship between the parties (i.e., whether agent-principal or otherwise), in compliance with RBI Directions 2025, Para 33.

a. Clear definition of outsourced activities and SLAs for performance and accountability
b. Provisions for continuous assessment and monitoring of the service provider to enable timely corrective actions.
c. Contingency plans to ensure business continuity in the event of service disruptions
d. Controls to ensure the confidentiality of customer data and stipulate the service provider's liability in case of security breaches or leakage of confidential information.
e. Provisions for prior approval from CA Grameen for the use of subcontractors by the service provider and ensure compliance with all relevant outsourcing directions.
f. Access to all books, records, and information relevant to the outsourced activity held by the service provider
g. The right to conduct audits of the service provider, whether by internal or external auditors, and to obtain copies of any related audit or review reports.
h. Clauses to recognize the right of supervisory authorities to inspect the service provider's books and accounts.

i. Clause obligating the service provider to comply with directions issued by supervisory authorities regarding the activities of CA Grameen
j. Termination clause specifying the conditions and minimum notice period required to execute termination
k. Clauses for preservation of data as per the regulatory and legal requirements
l. The Agreement shall specify the types of material adverse events and incident reporting requirements, including data breaches and service unavailability, and how these must be reported to CA Grameen
m. Events of default, indemnities, resolution processes, remedies, and recourse available to both parties
n. The Agreement shall specify the locations (regions or countries) where the outsourced services will be provided and where relevant data will be processed, including conditions for notifying CA Grameen of any changes in location
o. The Agreement shall adhere to RBI instructions on data storage
p. Clauses to ensure that cyber incidents / Security breaches or leakage of confidential information are reported to the CA Grameen by service provider without undue delay, so that the incident is reported by CA Grameen to the RBI within 6 hours of detection by the service provider

xviii. In case a Direct selling agent(s) or Direct Marketing agents or recovery agents are used:
a. A Board-approved code of conduct for DSAs, DMAs, and Recovery Agents is to be established, and their undertaking to follow it is to be obtained
b. Ensure that proper training is provided for DSAs, DMAs, and Recovery Agents to handle responsibilities with care, including customer solicitation, calling hours, privacy, and accurate product terms.
c. Training to be given to recovery agents to ensure that Intimidation, harassment, or actions that humiliate or intrude upon the privacy of debtors, guarantors, or their families are not engaged upon.
d. DSAs, DMAs, and Recovery Agents are also to be prohibited from sending inappropriate messages via mobile or social media, making threatening or anonymous calls, persistently calling, or making false/misleading representations
e. Steps are to be taken to ensure that calls for debt recovery are not to be made before 8:00 a.m. or after 7:00 p.m. to borrowers or guarantors. (Not applicable for MFI loans)

xix. CA Grameen shall ensure that the service provider will establish and maintain a business continuity framework, with joint testing conducted at least annually.

xx. CA Grameen will maintain sufficient control of the services to ensure operational continuity in case of sudden termination

xxi. Monitoring and Control:
a. CA Grameen shall conduct comprehensive pre- and post-implementation reviews of outsourcing arrangements and any material amendments thereto. Annual audits shall be conducted to assess the adequacy of the risk management practices in place for each outsourcing activity.

b. CA Grameen shall ensure reconciliation of transactions with service providers and sub-contractors, especially in cash management, according to RBI guidelines
c. CA Grameen shall document, and review Incentive compensation embedded in service provider contracts to prevent the encouragement of imprudent risks that could lead to reputational damage or other risks.
d. An annual compliance certificate, detailing outsourcing contracts, audit findings, and actions taken by the board, must be submitted to the supervisory authorities
e. The supervisory authorities must be notified immediately if significant outsourcing problems arise that could materially impact business operations, profitability, or reputation.
f. In cases of termination of service provider due to fraud, data leakage, breach of confidentiality, or blacklisting, public notices must be issued in newspapers, at branches, and on the company website. The details of the vendor will also be shared with Indian Banks' Association (IBA)/respective RBI-recognized Self-Regulatory Organizations (SROs). In addition, for all terminations of financial outsourcing agreements (regardless of the reason for termination), CA Grameen shall publicise the termination by displaying a notice at a prominent place in its branches, posting it on its website, and directly informing affected customers — so as to ensure that customers do not continue to deal with the service provider. This obligation applies to all terminations and is not limited to fault-based terminations (RBI Directions 2025, Para 44).
g. CA Grameen shall maintain an appropriate management structure for the ongoing monitoring and control of its outsourced financial activities and shall ensure that outsourcing agreements with service providers contain provisions to address this requirement.
h. Regular audits, by either the internal auditors or external auditors of CA Grameen shall assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, CA Grameen compliance with its risk management framework, and the requirements of these Directions.
i. CA Grameen shall maintain a central record of all material outsourcing of financial services for review by its Board and Senior Management. The records shall be updated promptly, and half yearly reviews shall be placed before the Board or Risk Management Committee.

xxii. CA Grameen shall implement a robust grievance redressal mechanism (where applicable), ensuring that outsourcing does not compromise this process. Responsibility for addressing grievances related to outsourced financial services shall remain with CA Grameen. Some of the parameters to be considered for grievance redressal mechanism are
a. Publicity should be given to the grievance Redressal mechanism by displaying it prominently at branches and on the website
b. The name, contact details (phone numbers and email address) of the designated grievance redressal officer, escalation matrix, and principal nodal officer

(wherever applicable) must be publicized widely

c. The designated grievance redressal officer should ensure prompt resolution of customer grievances.
d. The grievance redressal procedure and the time frame for responses should be available on the RE's website

xxiii. Additional Reporting:

a. CA Grameen Shall be responsible for Currency Transactions Reports and Suspicious Transactions Reports to FIU (Financial Intelligence Unit) or any other competent authority in respect of customer-related activities carried out by the service providers
b. All material financial outsourcing arrangements, including those involving extensive data sharing across geographic locations or when data related to Indian operations is processed abroad, should be reported to the supervisory authority on a quarterly basis as per the reporting format prescribed by RBI

xxiv. **Incentive compensation review**: The company shall also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider may, in certain instances of outsourcing, represent the company by selling products or services on its behalf, the company should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the company.

xxv. **Termination** : In the event of termination of an outsourcing agreement for any reason, this shall be publicised by CA Grameen by displaying at a prominent place in the branch, posting it on the website, and informing the customers so as to ensure that the customers do not continue to deal with the service provider.

12.8. Outsourcing within a Group / Conglomerate (Intra-Group Arrangements)

This section governs all outsourcing arrangements entered by CA Grameen with entities within its business group or conglomerate, for both financial and IT services, in compliance with RBI (NBFC – Managing Risks in Outsourcing) Directions, 2025, Para 45–51 and Para 90–92.

Board-Approved Policy and SLAs: Before entering any intra-group outsourcing arrangement (financial or IT), CA Grameen shall have a Board-approved policy specifically governing such arrangements and shall execute Service Level Agreements (SLAs) with the relevant group entities. These SLAs shall cover the scope of services, charges, demarcation of shared resources (e.g., premises and personnel), and

confidentiality of customer data.

Customer Transparency and Physical Demarcation: Where CA Grameen shares premises with group entities (including for cross-selling purposes), CA Grameen shall ensure that: (a) its entity identification is distinctly visible and clear to customers; (b) marketing materials used by the group entity and verbal communications by staff or agents within CA Grameen's premises shall clearly state the nature of the arrangement and the identity of the entity selling the product, so that customers are not confused about the seller; and (c) CA Grameen shall inform customers specifically about the company actually offering each product or service wherever multiple group entities are involved.

No Cross-Guarantee Representation: CA Grameen shall not publish any advertisement, enter into any agreement, or make any representation (express or implied) suggesting that CA Grameen is in any way responsible for the obligations of its group entities.

Operational Independence: CA Grameen shall ensure that its ability to carry out its operations in a sound fashion is not affected if premises or other services (such as IT systems and support staff) provided by group entities become unavailable. CA Grameen shall retain the ability to identify and manage risk on a stand-alone basis, and such arrangements shall not prevent RBI from obtaining information required for supervision of CA Grameen or the group.

Arm's Length and Identical Risk Management: CA Grameen shall, always, maintain an arm's length relationship with group entities. The risk management practices applied when outsourcing to a group entity (financial or IT) shall be identical to those applied for outsourcing to an unrelated third party. The selection of a group entity for IT services shall be based on objective criteria similar to those applied in the selection of an independent service provider, and any conflict of interest arising from such arrangement shall be appropriately addressed and disclosed.

Written Agreements: All intra-group outsourcing arrangements shall be appropriately documented in written agreements specifying scope of services; charges; confidentiality obligations for customer data; and a clear obligation for the group entity acting as service provider to comply with directions issued by RBI in relation to the activities of CA Grameen.

12.9. Offshore and Cross-Border Outsourcing

This section sets out specific requirements applicable to all outsourcing arrangements (financial and IT) where the service provider is located outside India, in compliance with RBI (NBFC – Managing Risks in Outsourcing) Directions, 2025, Para 52–53 and Para 93–94. These requirements are in addition to all other applicable provisions of this policy.

Eligible Jurisdictions: Outsourcing arrangements shall only be entered into with parties operating in jurisdictions that uphold confidentiality agreements and clauses. Before entering any offshore outsourcing arrangement, CA Grameen shall assess the political, social, economic, and legal environment of the jurisdiction and establish sound procedures for managing country risk, including appropriate contingency and exit strategies.

Governing Law: All offshore outsourcing agreements shall clearly specify the governing law of the outsourcing arrangement.

Availability of Records: CA Grameen shall ensure that the availability of records to CA Grameen and the RBI will not be affected even in the case of liquidation of the service provider or offshore custodian. CA Grameen shall retain the right — and ensure RBI also retains the right — to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction.

No Impediment to RBI Supervision: CA Grameen shall ensure that activities outsourced outside India are conducted in a manner that does not hinder efforts to supervise or reconstruct the activities of CA Grameen in a timely manner. Where the offshore service provider is a regulated entity, CA Grameen shall ensure that the relevant offshore regulator will neither obstruct the arrangement nor object to RBI inspections or visits by CA Grameen's internal or external auditors.

Protection from Offshore Regulatory Access and Jurisdiction: CA Grameen shall ensure that: (a) the regulatory authority of the offshore location does not have access to data relating to CA Grameen's Indian operations merely because processing is being undertaken at that offshore location; and (b) the jurisdiction of the courts in the offshore location where data is maintained does not extend to the operations of CA Grameen in India merely on the strength of the fact that data is being processed there, even though the actual transactions are undertaken in India.

Original Records in India: CA Grameen shall ensure that all original records continue to be maintained in India, irrespective of where processing is carried out. The offshore outsourcing arrangement shall comply with all statutory requirements and RBI regulations issued from time to time.

12.10. Pre-Outsourcing Evaluation for Material IT Outsourcing

Before initiating any material IT outsourcing arrangement (as defined in Section 12.3), CA Grameen shall carry out a formal pre-outsourcing evaluation in compliance with RBI (NBFC – Managing Risks in Outsourcing) Directions, 2025, Para 60. This evaluation shall be documented, approved by the appropriate authority as per the delegation framework, and shall cover the following four criteria:

(i) Need Assessment: An assessment of the need for outsourcing based on the

materiality and criticality of the IT activity to be outsourced. This shall consider whether the activity is core to CA Grameen's operations, whether internal capability exists or can be developed, and the strategic rationale for outsourcing versus in-house execution.

(ii) Expectations and Outcomes: A clear articulation of the expected outcomes and benefits from the outsourcing arrangement, including service quality targets, performance benchmarks, and how the arrangement supports CA Grameen's technology and business strategy.

(iii) Success Factors and Cost-Benefit Analysis: Identification of critical success factors for the arrangement and a formal cost-benefit analysis covering direct costs (contract value, integration, migration), indirect costs (internal oversight, compliance), and a comparison against the cost of retaining the activity in-house, including risk-adjusted costs.

(iv) Outsourcing Model: Determination of the appropriate outsourcing model (e.g., full outsourcing, co-sourcing, managed service, cloud service model), including a review of attendant risks and the availability of commensurate processes to manage those risks. The evaluation shall also confirm that appropriate governance and oversight capacity exists within CA Grameen before proceeding.

The pre-outsourcing evaluation shall be completed and documented prior to commencing the vendor selection or RFP process. The Risk Management function shall maintain a record of all such evaluations as part of the central IT outsourcing inventory.

13. Roles and Responsibilities

I. The Board of Directors and Senior Management are responsible for the overall implementation of this Policy and for ensuring that all outsourcing activities are conducted in accordance with its provisions.
II. The Risk Management function shall be responsible for developing and maintaining the vendor management framework and for producing the requisite templates (including due diligence checklists and periodic review templates) for use by the relevant business functions.
III. Each business function shall be responsible for vendor selection, classification, due diligence, onboarding, contingency planning, and periodic review in respect of vendors within its remit.
IV. The Risk Management function shall be responsible for maintaining the centralised vendor register and for overseeing initial due diligence and periodic review activities across all vendor relationships.
V. IT/Financial outsourcing.The relevant Head of Department shall be responsible for determining the materiality of any proposed IT or financial outsourcing arrangement.
VI. The Board or a Committee of the Board to which powers have been delegated, as applicable for financial or IT outsourcing, shall be responsible for putting in place a framework to evaluate the risks and materiality of all existing and prospective

outsourcing arrangements, laying down appropriate approval authorities depending on risks and materiality, and undertaking regular review.

VII. The Board, or a Committee of the Board to which powers have been delegated, shall be responsible for :

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the policies that apply to such arrangements
- Laying down appropriate approval authorities for outsourcing depending on risks and materiality;
- Setting up suitable administrative framework of Senior Management;
- Undertaking regular review of outsourcing strategies and arrangements for their continued relevance, and safety and soundness;
- Deciding on business activities of a material nature to be outsourced, and approving such arrangements;
- Approving a policy for outsourcing financial services to a group entity; and
- Reviewing records of all material outsourcing on half yearly basis, in which case the delegation should be to Risk Management Committee only.

VIII. In respect of outsourcing of IT services, the Board shall be responsible for :

- Putting in place a framework for approval of outsourcing activities depending on risks and materiality;
- Approving policies to evaluate the risks and materiality of all existing and prospective outsourcing arrangements;
- Setting up suitable administrative framework of Senior Management;
- Ensuring either by itself or through its Committee that there is no conflict of interest arising out of third-party engagements, especially when permitting an exception to the requirement that the service provider of outsourced services, if not a group company, shall not be owned or controlled by any director, key managerial personnel, approver of the outsourcing arrangement, or their relatives, as indicated under the proviso to paragraph 59 of these Directions; and
- Reviewing any adverse development mentioned in reports put up to Senior Management on the monitoring and control activities.

IX. The Audit Committee of the Board (ACB) shall:

- Monitor the system of internal audit of all outsourced activities; and
- Review the ageing analysis of entries pending reconciliation with outsourced vendors and make efforts to reduce the old outstanding items therein at the earliest.

X. **The IT Function shall be responsible for (in compliance with RBI Directions 2025, Para 64):**

- Assisting Senior Management in identifying, measuring, monitoring, mitigating, and managing the level of IT outsourcing risk within CA Grameen;
- Ensuring that a central database of all IT outsourcing arrangements (including key supply chain entities) is maintained, kept current, and is accessible for

review by the Board, Senior Management, internal and external auditors, and RBI supervisors;

- Effectively monitoring and supervising outsourced IT activities to ensure service providers meet laid-down performance standards and provide uninterrupted services; reporting findings to Senior Management; co-ordinating periodic due diligence reviews; and highlighting concerns or adverse developments as they arise; and
- Putting in place necessary documentation for all IT outsourcing contractual agreements, including service level management records, monitoring of vendor operations, key risk indicators (KRIs) for each material arrangement, and classification of vendors according to their determined risk level.

XI. Senior Management shall be responsible for creating essential capacity with required skillsets within CA Grameen to ensure proper oversight of outsourced IT services (RBI Directions 2025, Para 63(vii)). CA Grameen shall not outsource in a manner that depletes its internal capability to oversee and manage outsourced activities effectively. Where skill gaps are identified, Senior Management shall put in place a plan to develop or hire the necessary internal competencies.

XII. **Microfinance Loan – Specific Grievance Declaration (RBI Directions 2025, Para 56):** As an NBFC-MFI, CA Grameen shall ensure that a declaration is made in every microfinance loan agreement and in the Fair Practices Code (FPC) displayed at its offices, branch premises, and website, stating: (i) CA Grameen shall be accountable for any inappropriate behaviour of the employees of its service providers; and (ii) CA Grameen shall provide timely grievance redressal for any complaints arising from services rendered by outsourced agencies. The grievance redressal procedure, including the time frame for response (30 days from receipt of complaint), shall be published on CA Grameen's website. If a complaint is not resolved within 30 days or the complainant is not satisfied with the response, the complainant may escalate to the RBI's Integrated Ombudsman Scheme, 2021 (where applicable) or to the Consumer Education and Protection Cell (CEPC) of the relevant Regional Office of RBI.

XIII. **IT Outsourcing Termination – Customer Notification (RBI Directions 2025, Para 89):** In the event of termination of an IT outsourcing agreement for any reason, where the service provider has been dealing directly with customers of CA Grameen, the relevant function owner shall ensure that the termination is given due publicity so that customers cease dealing with the concerned service provider. Such publicity shall be provided through appropriate channels (branch notices, website, and direct customer communication where applicable) and shall be co-ordinated by the function owner in consultation with the Compliance and Communications teams. This obligation applies to all terminations regardless of the reason for termination.