CREDITACCESS GRAMEEN LIMITED

Vendor & Outsourcing Management Policy

Version 2.1

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

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

Contents

1. Introduction

We outsource various services to reduce costs as well as to avail specialist expertise not available internally. Vendor Management is the process of ensuring that the use of service providers and suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance while outsourcing any of our services. The purpose of this document is to define a framework for outsourcing and driving vendor management program within CA Grameen during the entire lifecycle of outsourcing w.r.t; Initiation till 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 framework specifies the requirements for establishing, implementing, maintaining, and continually improving a Vendor Management system aligned to outsourcing various services. This policy outlines the assessing materiality of outsourcing specific services based on certain key factors. This framework includes requirements for the assessment and treatment of vendor related risks as per the needs of the organization. This framework will act as a guiding document to the Top Management, Purchase Committee, members of Information Security team, users of the business units, vendors, third-party employees who are involved in Vendor Management across the organization irrespective of the location of office/branches of CAGrameen. The policy will also ensure that the values of CA Grameen with regards to the environmental standards, human

rights, and ethical business practice is being followed by the suppliers and all their personnel

5. Principles of Vendor Risk Management

CA Grameen is committed to the ethical establishment, implementation, and maintenance of service outsourcing process. CA Grameen shall ensure protection of information belonging to clients, licensees and their clients, employee information, and all other proprietary information held within the CA Grameen information processing facilities and systems while the services are outsourced to third party. Vendor Management Policy provides the management's directive towards vendor management. The policy shall be communicated within the organization and shared with interested parties, as appropriate, after necessary approvals.

The salient principles are as follows:

a. Establish a fair system that allows unbiased opportunities to all third parties.
b. Establish roles and responsibilities for vendor Management
c. Ensure that all risks related to outsourcing are addressed/considered prior vendor onboarding and continuous monitoring of the risks and their remediations are performed via periodic assessments.
d. Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the vendor management process.
e. Ensure that all third parties involved in vendor management have to adhere to the relevant legal and regulatory requirements through legally enforceable contracts
f. Ensure that policies, standards, procedures, and guidelines are developed, reviewed, and updated for the implementation of vendor management

6. Vendor's Code of Conduct

6.1. Environment Sustainability

i. Suppliers shall follow all laws of the land including laws on Environment sustainability and protection while executing any work for the Company.
ii. Establish operational practices which minimize the impact on the environment and deploy measures to prevent and reduce harm to the environment.
iii. Efficient use of natural resources and application of energy-efficient, environment-friendly technologies and reduction of waste as well as emissions to air, water, and soil.
iv. Comply to waste segregation and disposal rules laid down by the center/state/local authorities.
v. Work actively to improve the environment in the communities in which they operate and minimize their impact on biodiversity, climate change.

6.2. Social Responsibility

i. The supplier shall comply with all local employment, labour laws, and laws regarding human rights in the operating geographies.
ii. Supplier shall commit to eliminating any kind of forced labour & child labour.
iii. Suppliers shall provide their employees with a workplace free of harsh and inhumane treatment, without any sexual harassment, sexual abuse, corporal punishment or torture, mental or physical coercion or verbal abuse of employees, or the threat of any such treatment.
iv. Suppliers will provide a safe working environment through proactive management and controls that minimize health and safety risks and support accident prevention.
v. All employees should be paid a fair wage commensurate with prevailing industry conditions or the minimum wage, whichever is higher.
vi. Suppliers shall ensure that their employees have a mechanism to report grievances and that facilitates open communication between management and employees. Being responsible for employee compensation and payment of fair wages.
vii. Suppliers must provide a work environment that is free of discrimination based on race, color, age, gender, sexual orientation, ethnic origin, religious beliefs, political views, or any other prohibited ground. Their staff recruitment practices must also comply with the principle of equal opportunities for similar skills.

7. Vendor Management / Governance Process

7.1. Discovering a business need

i. The respective function determines whether it needs to improve an existing process, reduce costs, or create a new product.
ii. Once the need is identified, a cost-and-benefit analysis is undertaken. A decision is made to either use internal resources or outsource the work. Organizations usually seek outside help because they believe the vendor can do the work faster, better, and/or at a lower cost
iii. The decision to use a vendor (to outsource an activity) should be in line with long term strategic interest of the company and shouldn't lead to undue increase in risk profile of the company
iv. Materiality of outsourcing of an activity is to be assessed by the Head of departments prior to making Financial / IT outsourcing decision.
v. Materiality of the outsourced activity should be calculated on gross basis based on
    a. Importance of outsourced activity to the organization. The importance is determined based on percentage of customers or revenue covered by the activity
    b. The potential impact of outsourcing on solvency, liquidity, capital and impact to 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. Aggregate risk of using the same service provider for multiple outsourcing activities
f. Impact on customer service due to outsourcing the activities
g. The degree of difficulty, including the time required, in finding an alternative service provider or bringing the activity in-house.
h. Impact to financial market and counterparties of the organization if the service provider fails to perform the services

vi. If the overall risk identified based on the materiality is considered high, then the final decision for outsourcing the activity needs to be approved by the board

7.2. Developing the scope of work

i. Make sure that the scope of work syncs with the need's assessment determined in the first stage.
ii. CA Grameen should maintain a list of vendors in a central location, review that list to see if it makes sense to expand the relationship with an existing vendor rather than hire a new one.

7.3. Issuing request for proposals (RFP)

i. To ensure CA Grameen select the best vendor, the respective function shall float request for proposals and information from vendors in cases of critical and significant categories of vendors / outsourcing activity.
ii. If the vendor is expected to handle a core business process, a cross-functional team shall be formed to finalize the RFP.
iii. An Software Bill of Material (SBOM) must be mandatorily collected during the procurement of any critical software or application. Vendors should be required to demonstrate their SBOM generation process and provide SBOMs that can be validated for completeness and accuracy, including clear listing of dependencies and open-source components.
iv. The SBOM Should contain minimum of the following:
    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. Be aware of increased vulnerability in the areas of strategic, reputation, compliance, transaction, operational, social media, credit, and other risks. The subsequent sections shall provide additional guidance on due diligence.
ii. Specific importance shall be given to understand how vendor deals with sensitive customer information and whether these meets required regulatory norms
iii. Vendor must disclose if any employee or director of CA Grameen holds direct or indirect interest with the vendor
iv. The SBOM collected from the vendors is to be reviewed and approved by the Information security team for any security gaps.

7.5. Selection of Vendor

i. The respective HOD shall evaluate all proposal and select a vendor for the proposed work
ii. The vendor should be evaluated based on objective criteria to the extent possible
iii. HOD shall obtain necessary approval as per the laid down expense approval procedure

7.6. Negotiating contracts for critical / significant vendors

i. Respective functions should ensure that the contract includes information security

clauses. The function may seek necessary support from the Information Security team in this regard.

ii. The right to audit the vendor and their subcontractors for outsourced partners.

iii. The contract should require the vendor to notify CA Grameen if the vendor experiences financial difficulty, catastrophic events, information security incidents, a change in its strategic goals, or significant staffing changes.

iv. By including exact, quantifiable parameters along with clearly defined scope of work in the contract, one can establish clear expectations regarding the vendor's responsibilities

v. The contract should also specify consequences if the expectations are not met. If incentives for superior performance are to be awarded, they should be included in the contract. A clearly defined exit clause should be in place.

vi. Background checks, non-disclosure and security policy compliance agreements shall be in place

vii. Should include clauses on audit trails, record retention and evidencing

viii. Should clearly specify payment terms, escalation /complaint mechanism etc.

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 respective function needs to periodically monitor the vendor's performance, assess the risk.(Refer Section 11)

ii. Even if the line of business manages the vendor's performance, key information about the vendors should be kept in a centralized location i.e. vendor inventory. (Refer Section 10)

iii. Respective function shall consider developing KPI's to monitor the performance of vendors wherever feasible, and this should be presented during periodic review. Annual review of SBOM should also be considered while reviewing a critical software / application vendor

iv. Changes in services provided by suppliers should be agreed only after a thorough review including assessment of any information security implications so that the effectiveness of controls is maintained.

7.8. Terminating or Renewing Contracts

i. Respective functions shall renew contract after reviewing the business need for the vendor and determine whether CA Grameen needs to outsource or can build inhouse capability

ii. Based on the vendor's performance and existing market competition, it may be more

advantageous to continue with the existing vendor or to create a new relationship (without a service disruption)

iii. Respective functions shall have a contingency plan in case the vendor becomes unreliable, and the relationship needs to be discontinued.

iv. Respective functions shall ensure Vendor contracts after termination are archived and maintained to meet the regulatory requirements.

8. Vendor Categorization

Vendors shall be categorized into three levels

i. **Critical** - Vendors are categorized as critical if they can cause significant financial loss or can lead to business disruptions beyond 24 hours or lead to reputational loss or regulatory non-compliance if they fail to deliver services as promised, or if they are breached. Example: data center, application vendors etc.

ii. **Significant** – Significant vendors are those that provide services to CA Grameen, managing the inner workings of our business so it runs as efficiently as possible. In the event of failure, the impact is limited to monetary impact in the form of efficiency loss or disruptions less than 24 hours. Example: ISP etc.

iii. **Non-essential** - If a break in the supply chain occurred, alter55native can be arranged promptly and there would be little or no consequences to maintaining service levels and customer service. Example: Office Supplies

9. Risk Assessment at Onboarding

i. A due diligence must be performed on one or more of the likely selected vendors. The depth of the due diligence may vary according to the relative importance of the vendor relationship, but it should cover the following areas:

   a. Existence and corporate history. Vendor's business history and market share
      for a given service
   b. Financial strength, solvency to carry out the task/project with satisfaction
   c. Dependency on key employees, whether loss of 1-2 employees can put the delivery at risk
   d. Qualifications, backgrounds and reputations of company principals, including criminal background checks where appropriate
   e. Vendor's reputation (including adverse media reports) and past performance
      with similar business partners
   f. Vendors experience and competence to implement and support the outsourced activity over the contracted period & its ability to provide services to all customers with confidentiality (mandatory for financial outsourcing)
   g. **Internal control environment-** Consider reviewing their audit reports,

internal control evaluations and assessments of the third parties as per the business applicability.

h. **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)
i. **Compliance risk** including any regulatory actions taken and/or anti-bribery corruption risk
j. Reliance on and success in dealing with third party service providers.
k. The type of access the third party will have to CreditAccess Grameen's
information assets and the value and sensitivity of information involved.
l. 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 employee/ Director has a direct or indirect interest on 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)

ii. A detailed checklist will be maintained by the risk department covering all risk areas and will be shared with the respective department Head's / vendor mangers during onboarding.

iii. The extent of due diligence may vary depending on the vendor classification as per matrix 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. An inventory of vendors shall be maintained centrally which shall include name, description, categorization by criticality, last review details and relationship owner. The list must always be up to date.

ii. A centralized Inventory of IT and financial activities outsourced to service providers (including key entities involved in their supply chains) will also be maintained.

11. Periodic Review of Vendor Risk

i. Periodic review of vendor shall be done by the respective vendor relationship owner. The review shall include at a minimum:

   a. **Counterparty Risk** - Whether the vendor has delivered as per expectation since the last review or there were clearly identifiable deficiencies
   b. **Compliance & Contractual Risk:** Was there a breach in contract or compliance / regulatory requirements and actions taken against the vendor
   c. **Jurisdictional risk & Country risk**– current political, social or legal climate of the service providers jurisdiction / country
   d. Is there a documented exit strategy for the vendor & over reliance of same vendor for multiple services (Only for critical vendors)
   e. **Strategic risk:** Whether the vendor provides its services consistent with the overall strategic directive of the company (Only for financial outsourcing)
   f. Deterioration in financial situation since last review and if this is material in nature
   g. Change in management or Loss of key personnel that can impact the delivery
   h. Any cyber security incident in vendor site; observation from of IT audit report
   i. Any adverse media report (print or social media) that can impact delivery or can have associated reputational harm to CAGL.
   j. Whether respective function has a contingency plan in place in case of disruptions at the vendor end (applicable for critical vendor only)

k. Whether CA Grameen employee or director has Direct / Indirect interest on the vendor
l. **Operational risk**: Any operational continuity risk arising from outdated technology used, Inadequate process to perform activities (If applicable), frauds and errors (if any) that occurred during the review period. (This will be primarily applicable to financial outsourcing)
m. **Reputation risk**: whether the service provided & customer interaction by the service provider is adequate with the companies standard and meets the confidentiality requirements in terms of customer interaction (Only for financial outsourcing)
n. Whether there is an detailed SBOM in place and is periodically updated for critical software /application.

ii. A detailed list will be maintained by risk team covering all risk area to be assessed during periodic review and this will be shared to the respective département head's / vendor owners as and when its needed.

iii. When to perform periodic review
a. Outsourced services will be considered as critical vendors, and a half yearly review of financial outsourced services must be performed additional to the periodic risk assessment as per 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

Outsourcing is defined as company's use of a third party (either an affiliated entity within a group or an external entity) to perform activities that would normally be undertaken by the CAGL itself on a continuing basis, now or in the future.

This section primarily talks about 2 types 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

The following are the list of activities that cannot be outsourced as per the RBI Regulations:

i. Core management functions, including policy formulation and significant decision-making processes like determining compliance with KYC norms

ii. Loan Sanctioning
    a. The final decision to extend credit must be made internally, not by an outsourced service provider.
    b. Even with a pre-defined loan sanctioning template (Approved by the board), it must be demonstrated that the decision to lend was made solely internally, with the service provider acting only as a facilitator.

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. Guidelines for IT Services Outsourcing

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

i. CA Grameen shall ensure that outsourcing should neither impede nor interfere with the CA Grameen ability to effectively oversee and manage its activities. Further that the outsourcing should not impede RBI in carrying out its supervisory functions & objectives.

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.

iii. Risk assessment will be carried out prior to initiating outsourcing and identified risks shall be monitored on an ongoing basis.

iv. Mitigation action/s needs to be worked out for events leading to Business disruptions, customer data leakage and backup failures.

v. In considering or renewing an Outsourcing of IT Services arrangement, appropriate due diligence shall be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis.

vi. All IT outsourcing contracts will include at minimum the following.
    a. Requirements to be met/provided by the outsourced service providers.
    b. Clear definition of services.
    c. Scope of services to be provided.
    d. Qualification requirements for personnel including but not limited to training and, competency requirements.
    e. Screening requirements for outsourced service provider personnel.
    f. Roles and responsibilities
    g. Performance requirements or SLA's
    h. Communication processes.
    i. Resilience, recovery, and contingency arrangements including business continuity requirements.
    j. Definition of changes and process for managing changes.
    k. Payment terms including criteria for service credits.
    l. 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.
    m. Retention of requisite audit trails and logs for administrative activities carried out by the outsourced service providers as applicable.
    n. Periodic reviews with vendors against the agreement/contract.
    o. Definition of complaints and process for complaint management.
    p. Processes for escalation management.
    q. Process for dispute management.
    r. Process for incident reporting and subsequent action including corrective

actions.

s. 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
t. Right to audit clauses allowing audit by CA Grameen directly, their appointed auditors, statutory and regulatory auditors such as those from RBI.
u. Right to access necessary records and evidence as necessary based on approved requests.
v. Record retention and evidencing.
w. Non-disclosure agreements/confidentiality agreements.
x. Clearly defined exit clauses.
y. Risk of unexpected termination of the outsourcing contract / agreement or liquidation of outsourced service providers.
z. Notify RBI or any other relevant authority in the event of security breach or leakage of confidential information relating to CA Grameen's customer.
aa. Liability for damages on security breach or leakage of customer data.

vii. It shall be ensured that clarity is available on the data flows and responsibility for the data flows between CA Grameen and the outsourced service providers.

viii. A single point of contact will be allocated for all outsourced service providers to enable effective outsourced entity management.

ix. Outsourced service providers will be required to inform CA Grameen of all planned/proposed sub-contracting proposed by them during the course of service provision. Suitable risk assessment and mitigation action/s needs to be worked out before approval for such sub-contracting activities. The risk assessment amongst other aspects needs to specifically consider events leading to BCP /DR situations, data protection and backup arrangements, liability for damages on security breach or leakage of customer data and costs for CA Grameen / outsourced service providers to take the sub-contracted activity into their fold for continuing the services.

x. Periodic monitoring of service provided, and reporting requirements shall be documented and agreed upon.

xi. It shall be ensured that necessary corrections and corrective actions shall be initiated on any violations/deviations observed relating to the overall 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. There will be a separate Exit strategy for IT outsourcing vendor documented and approved by respective function head

12.3. Requirements for cloud computing solutions

In addition to the Outsourcing of IT Services controls prescribed above, CA Grameen shall check / validate the following requirements for storage, computing, and movement of data in cloud environments.

i. While considering adoption of cloud solution, it is imperative to analyse the business strategy and goals adopted to the current IT applications footprint and associated costs. Cloud adoption ranges from moving only non-business critical workloads to the cloud to moving critical business applications such as SaaS adoption and the several combinations in-between, which should be based on a business technology risk assessment.

ii. In engaging cloud services, CA Grameen shall ensure, inter alia, that the Outsourcing of IT Services policy addresses the entire lifecycle of data, i.e., covering the entire span of time from generation of the data, its entry into the cloud, till the data is permanently erased/ deleted. The CA Grameen shall ensure that the procedures specified are consistent with business needs and legal and regulatory requirements.

iii. In adoption of cloud services, CA Grameen shall take into account the cloud service specific factors, viz., multi-tenancy, multi-location storing/ processing of data, etc., and attendant risks, while establishing appropriate risk management framework. Cloud security is a shared responsibility between the CA Grameen and the Cloud Service Provider (CSP).

iv. 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.

v. 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.

vi. 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.

vii. Security Considerations

a. Service and Technology Architecture: CA Grameen shall ensure that the service and technology architecture supporting cloud-based applications is built in adherence to globally recognized architecture principles and standards. CA Grameen shall prefer a technology architecture that provides for secure container-based data management, where encryption keys and Hardware Security Modules are under the control of the CA Grameen.

b. 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.

c. 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 application

d. Robust Monitoring and Surveillance: CA Grameen shall accurately define minimum monitoring requirements in the cloud environment.

e. 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.

f. 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.

viii. 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.

12.4. Guidelines for Financial Services Outsourcing

In addition to the guidelines prescribed above for Vendor management, the following controls will also be applicable additionally if the activity is categorized as financial 3 outsourcing as per the definition given in the policy

i. 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.

ii. 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

iii. 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.

iv. CA Grameen shall ensure that service provider staff's access to customer information is strictly to what is necessary for performing the outsourced function.

v. 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

vi. 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.

vii. 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

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

ix. In case agents are used for sales, marketing etc, CA Grameen shall clearly state in financial product literature or brochures that agents may be involved in sales or marketing of financial products and describe the role of these agents in broad terms.

x. 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.

xi. All Financial outsourcing contracts will include at minimum the following.
    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

xii. 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)

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

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

xv. Monitoring and Control:

a. CA Grameen shall perform a comprehensive pre- and post-implementation reviews of outsourcing arrangements or amendments. Annual audits should also be performed to assess the adequacy of risk management practices put in please for outsourcing activities.

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)

xvi. 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

xvii. 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

xviii. **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.

13. Roles and Responsibilities

I. The board and senior management are responsible for overall implementation of this policy
II. Risk management shall be responsible for development and updation of vendor management framework and shall develop necessary templates (due diligence, periodic review etc.) to be used by the relevant functions.
III. Respective functions shall be responsible for vendor selection, classification, due diligence, on-boarding, contingency planning and periodic review of the vendor.
IV. Risk Management shall be responsible for maintaining centralized vendor inventory, monitor initial due diligence and monitor periodic review of vendors.