CREDITACCESS GRAMEEN LIMITED

Vendor Management Policy

Revision History

Version	Author	Description of Changes	Release Date
1	Loyal Quadras DGM – Risk Mahantesh Dhangi, Information Security Manager	First version	March 23, 2022

Version	Author	Reviewed by	Approved by
1	Loyal Quadras DGM – Risk Mahantesh Dhangi, Information Security Manager	Firoz Anam Chief Risk Officer Sudesh Puthran Chief Technology Officer	Board of Directors

Contents

1 Introduction 4

2 Scope 4

3 Principles of Vendor Risk Management 4

4 Vendor's Code of Conduct 5

5 Vendor Management / Governance Process 5

6 Vendor Categorization 7

7 Risk Assessment at Onboarding 7

8 Vendor Inventory 8

9 Periodic Review of Vendor Risk 8

10 Roles and Responsibilities 9

1 Introduction

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.

The purpose of this document is to define a framework for driving vendor management program within CA Grameen during the entire lifecycle of outsourcing w.r.t; Initiation till Termination.

2 Scope

This framework specifies the requirements for establishing, implementing, maintaining, and continually improving a Vendor Management system. 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 CA Grameen. The policy will also ensure that the values of CA Grameen with regards to the environmental standards, human rights, and ethical business practice are being followed by the suppliers and all their personnel.

3 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:

- Establish a fair system that allows unbiased opportunities to all third parties.
- Establish roles and responsibilities for vendor Management
- 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.
- Provide sufficient resources to establish, implement, operate, monitor, review, maintain and improve the vendor management process.
- Ensure that all third parties involved in vendor management have to adhere to the relevant legal and regulatory requirements through legally enforceable contracts
- Ensure that policies, standards, procedures, and guidelines are developed, reviewed, and updated for the implementation of vendor management

4 Vendor's Code of Conduct

Environment Sustainability

a) Supplier shall follow all laws of the land including laws on Environment sustainability and protection while executing any work for the Company.
b) Establish operational practices which minimize the impact on the environment and deploy measures to prevent and reduce harm to the environment.
c) 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.
d) Comply to waste segregation and disposal rules laid down by the center/state/local authorities.
e) Work actively to improve the environment in the communities in which they operate and minimize their impact on biodiversity, climate change.

Social Responsibility

a) The supplier shall comply with all local employment, labour laws, and laws regarding human rights in the operating geographies.
b) Supplier shall commit to eliminating any kind of forced labour & child labour.
c) 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.
d) Suppliers will provide a safe working environment through proactive management and controls that minimize health and safety risks and support accident prevention.
e) All employees should be paid a fair wage commensurate with prevailing industry conditions or the minimum wage, whichever is higher.
f) 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.
g) Suppliers must provide a work environment that is free of discrimination based on race, colour, 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.

5 Vendor Management / Governance Process

a) Discovering a business need
    i. The respective function determines 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
b) 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.

c) 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.
   ii. If the vendor is expected to handle a core business process, a cross-functional team shall be formed to finalize the RFP.

d) 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

e) 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

f) Negotiating contracts for critical / significant vendors:
   i. Respective functions should ensure that the contract includes information security clauses.
   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 exist 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.

g) Monitoring Performance
   i. The respective function needs to periodically monitor the vendor's performance, assess the risk (Refer Section 8)
   ii. Even if the line of business manages the vendor's performance, key information about the vendors should be kept in a centralized location (Refer Section 7).
   iii. Respective function shall consider developing KPI's to monitor the performance of vendors and this should be presented during periodic review
   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.

h) 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.

6 Vendor Categorization

Vendors shall be categorized into three levels

1. **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.
2. **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, HRIS etc.
3. **Non-essential** - If a break in the supply chain occurred, alternative can be arranged promptly and there would be little or no consequences to maintaining service levels and customer service. Example: Office Supplies

7 Risk Assessment at Onboarding

a) 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:
   i. Existence and corporate history. Vendor's business history and market share for a given service
   ii. Financial strength, solvency to carry out the task/project with satisfaction
   iii. Dependency on key employees; whether loss of 1-2 employees can put the delivery at risk
   iv. Qualifications, backgrounds and reputations of company principals, including criminal background checks where appropriate
   v. Vendor's reputation (including adverse media reports) and past performance with similar business partners
   vi. Internal control environment. Consider reviewing their audit reports, internal control evaluations and assessments of the third parties as per the business applicability.
   vii. Legal and compliance including any regulatory actions and/or anti-bribery corruption risk
   viii. Reliance on and success in dealing with third party service providers. The type of access the third party will have to CreditAccess Grameen's information assets and the value and sensitivity of information involved.
   ix. Insurance coverage. Ensure that the vendor has sufficient coverage to insure against losses due to dishonest acts, and liability coverage for losses due to negligent acts.
   x. Ability to comply with information security requirements

xi. Ability to meet disaster recovery and business continuity requirements.
xii. Whether employee/ Director has a direct or indirect interest on the vendor

b) The extent of due diligence may vary depending on the vendor classification as per matrix below

Parameter	Critical	Significant	Non-essential
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
Third Party Reliance	Y		
Reputation	Y	Y	Y
Insurance Coverage	Y		
Anti-Bribery / Corruption	Y	Y	Y

8 Vendor Inventory

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 be up to date at all times.

9 Periodic Review of Vendor Risk

a) Periodic review of vendor shall be done by the respective vendor relationship owner. The review shall include at a minimum:
- Whether the vendor has delivered as per expectation since the last review or there were clearly identifiable deficiencies
- Deterioration in financial situation since last review and if this is material in nature
- Change in management or Loss of key personnel that can impact the delivery
- Any cyber security incident in vendor site; observation from of IT audit report
- Any adverse media report (print or social media) that can impact delivery or can have associated reputational harm to CAGL
- Whether respective function has a contingency plan in place in case of disruptions at the vendor end (applicable for critical vendor only)
- Whether CA Grameen employee or director has Direct / Indirect interest on the vendor.

b) When to perform periodic review

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

10 Roles and Responsibilities

- 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.
- Respective functions shall be responsible for vendor selection, classification, due diligence, on-boarding, contingency planning and periodic review of the vendor.
- Risk Management shall be responsible for maintaining centralized vendor inventory, monitor initial due diligence and monitor periodic review of vendors.