POLICY FOR OUTSOURCING OF FINANCIAL SERVICES

Standard Capital Markets Limited

Table Of Contents

DOCUMENT IDENTIFICATION INFORMATION

Document Name	Policy for Outsourcing of Financial Services
Index	Scale Based Regulations/ Compliance/Outsourcing of Financial Services
No. of Pages	24
Approving Authority	Board of Directors
Review Frequency	Annually or earlier, if warranted by any regulatory changes, operational requirements, or business needs, to ensure its continued suitability, adequacy, and effectiveness in alignment with applicable laws, guidelines, and the Company's objectives.

This policy is issued by Standard Capital Markets Limited (hereinafter referred to as "SCML" or "Company") and encompasses all affiliated entities, employees, and stakeholders associated with SCML's operations.

1. BACKGROUND

1.1. Standard Capital Markets Limited has adopted this Outsourcing of Financial Services Policy (hereinafter referred to as "Policy") in compliance *with Clause 48 and Annex XIII of the Master Direction – Reserve Bank of India (Non-Banking Financial Company – Scale-Based Regulation) Directions, 2023, dated October 19, 2023.*

1.2. The Policy outlines the principles, due diligence requirements, risk mitigation measures, and governance mechanisms that must be adhered prior to and during the course of outsourcing any financial services.

1.3. The Policy ensures that all outsourcing engagements are undertaken in a manner that does not diminish the Company's ability to fulfil

its regulatory obligations, compromise the interests of its customers, or impair the integrity of its operations.

1.4. The Company affirms that outsourcing of financial services will not result in the transfer of its core management functions or regulatory accountability. The Company shall retain ultimate control, oversight, and responsibility for all outsourced activities, regardless of whether they are performed by group entities or unrelated third parties.

2. DEFINITIONS & INTERPRETATIONS

Unless otherwise defined by the RBI in its various directions, guidelines issued from time to time or apparent from the context, the following terms shall have the meaning as assigned herein below, and cognate expressions shall be construed accordingly

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

2.2. "Continuing Basis" encompasses agreements with the Service Provider for both indefinite and limited periods, where the services are performed repeatedly or continuously over time.

2.3. " Outsourced financial services" typically include, but are not limited to, the processing of applications (such as loan origination, credit card), document processing, marketing and research, loan supervision, data processing, recovery processes and back-office operations.

2.4. "Material outsourcing arrangements" are defined as those which, if disrupted, could significantly impact the Company's business operations, reputation, profitability, or customer service.

2.5. "Service Provider" shall mean any person or entity appointed or proposed to be appointed by the Company to carry out the

outsourcing activities that may either be a member of the group/conglomerate to which the Company belongs or an unrelated party.

2.6. "Senior management" means personnel of the company who are members of its core management team excluding Board comprising all members of management one level below the executive directors, including the functional heads i.e. head of Functional departments.

2.7. "Customer" shall mean any existing or prospective customers of the Company.

2.8. "Functional Department" shall mean the specific department of the Company undertaking any Business Function within the organization, and whose head shall be designated as Functional Head.

2.9. "Committee" shall mean any committee constituted by the Board from time to time.

2.10. "Confidential Information" means all proprietary, sensitive, or non-public information relating to the Company, its holding company, subsidiaries, affiliates, or licensees, including customer information, business data, financial records, documents, models, processes, policies, and any information, whether in physical or electronic form, the disclosure of which may adversely impact the Company or its stakeholders.

3. SCOPE & APPLICABILITY OF THE POLICY

3.1. This Policy applies to all outsourcing arrangements entered into by the Company for financial services, whether with affiliated entities within the same corporate group or with external third-party service providers.

3.2. These instructions are specifically intended to address and manage the risks arising from the outsourcing of financial services. Accordingly, this Policy shall not apply to outsourcing arrangements pertaining to non-financial support services which do not impact the

Company's financial business. Such excluded activities shall include, but shall not be limited to, courier services, staff catering, housekeeping and janitorial services, security of premises, and movement or archiving of physical records.

3.3. The Company further affirms that no prior approval from the RBI is required for entering into outsourcing arrangements for financial services. However, all such arrangements shall remain subject to inspection, scrutiny, and both on-site and off-site monitoring by the RBI, and the Company shall ensure full compliance with all regulatory requirements in this regard.

3.4. The Policy shall apply to material outsourcing by service provider(s) and equally to activities subcontracted by the service providers.

4. OBJECTIVE OF THE POLICY

4.1. The purpose is to ensure that all outsourced activities and services of the Company are managed effectively, with due regard to risk, compliance, and borrower's interest. Specifically, the policy aims to:

4.1.1. Safeguard customer interests by ensuring that outsourced activities are carried out in a secure, transparent, and compliant manner.

4.1.2. Guarantee that both the Company and the RBI have unrestricted access to all relevant books, records, and information maintained by service providers.

4.1.3. Uphold the integrity, accountability, and operational standards of the Company in all outsourced functions

5. NON-OUTSOURCEABLE ACTIVITIES

5.1. The Company shall not outsource its core management functions, including but not limited to:

5.1.1. Internal Audit

5.1.2. Strategic Management Functions

5.1.3. Compliance Functions

5.1.4. Decision-making functions such as:

5.1.4.1. Determining compliance with Know Your Customer (KYC) norms

5.1.4.2. Sanctioning of loans, including retail loans

5.1.4.3. Management of the investment portfolio

5.2. These Core functions shall remain within the direct ownership, supervision, and control of the Company to ensure adherence to regulatory obligations, accountability, and risk oversight

5.3. In the case of the Company forming part of a group or financial conglomerate, core management functions may be outsourced within the group, subject to strict compliance with the conditions stipulated hereby in the policy or any directions issued by the regulatory authorities as amended from time to time. Such intra-group outsourcing shall also adhere to all controls and safeguards specified under this Policy, including those relating to risk management, confidentiality, independence, and oversight, to ensure that the Company retains ultimate responsibility and accountability for the outsourced functions.

5.4. The Company shall not outsource the internal audit function in its entirety. However, the Company may engage external experts or professionals on a contractual basis to assist in carrying out specific audit tasks, subject to the condition that such engagement does not compromise the independence, objectivity, or effectiveness of the internal audit process. The performance, competence, and effectiveness of external experts or professionals engaged for internal audit support shall be periodically reviewed by the Board.

6. CALSSIFICATION CRITERIA FOR MATERIAL OUTSOURCING

6.1. An outsourced activity shall be classified as material based on the following qualitative and quantitative parameters:

Qualitative Parameters	The Functional Head shall assess and identify material outsourcing arrangements where:

	❖ The Company depends on the service provider for critical financial functions such as continuous processing of loan applications, customer onboarding, verification, or approval workflows; ❖ Failure or inefficiency on the part of the service provider to perform services as per the agreed standards can significantly affect the Company's solvency, liquidity, earnings, funding capital, or overall risk profile; ❖ The activity outsourced is central to the achievement of the Company's strategic objectives and failure may materially damage its brand reputation or market standing; ❖ The cost, time, and operational disruption involved in replacing the service provider would be substantial ❖ The outsourced activity involves access to or processing of customer data or confidential Company information, thereby posing risks to data security and customer privacy; ❖ There is significant dependency or concentration of functions outsourced to a particular service provider across multiple processes or geographies.
Quantifiable Parameters	An outsourced activity may also be classified as material if the cost of outsourcing activity is exceeding the Company's total operating expenses for the previous financial year;

6.2. The Functional Head of each relevant business or operational unit shall be responsible for evaluating and classifying outsourced activities as 'Material' or 'Non-Material' and shall ensure that such classification is documented, justified, and periodically reviewed.

6.3. All Material Outsourcing arrangements must be subject to enhanced due diligence, contract structuring, business continuity planning, and periodic performance assessments in line with this Policy.

6.4. Non-Material Outsourcing arrangements may also be reviewed periodically to assess emerging materiality risks or dependency concerns.

7. GOVERNANCE FRAMEWORK

7.1. The Company acknowledges that the outsourcing of any activity shall not diminish its obligations, nor those of its Board and Senior Management, who shall remain ultimately responsible and accountable for the outsourced activity.

7.2. The Company shall retain full control over all outsourced functions and shall be liable for the actions, omissions, and performance of the service providers, including but not limited to DSAs, DMAs, and recovery agents. The confidentiality and integrity of customer information shared with service providers shall be strictly preserved.

7.3. The Board of Directors is responsible for:

7.3.1. Approving the framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements, along with the associated policies.

7.3.2. Establishing appropriate approval authorities for outsourcing based on the assessed risks and materiality.

7.3.3. Setting up a suitable administrative framework of senior management for implementing the outsourcing arrangements.

7.3.4. Undertake regular reviews of outsourcing strategies and arrangements to ensure their continued relevance, safety, and soundness.

7.3.5. Deciding on and approving business activities of material nature to be outsourced.

7.4. The Senior Management of the Company shall be responsible for:

7.4.1. Evaluating risks and materiality of all existing and prospective outsourcing arrangements in pursuance of this Policy;

7.4.2. Developing and implementing outsourcing policies and procedures in consonance with the nature, scope, and complexity of the outsourcing activity;

7.4.3. Periodically reviewing the effectiveness of policies and procedures of the Company concerning the outsourcing of financial services;

7.4.4. Ensuring timely communication of risk-related information concerning material outsourcing arrangements to the Board;

7.4.5. Ensuring that the contingency plans concerning realistic and probable disruptive scenarios are proper and adequately tested;

7.4.6. Overseeing independent reviews and audits to ensure compliance with established policies;

7.4.7. Undertake a review of outsourcing arrangements periodically to ensure timely identification of new material outsourcing risks.

8. RISK ASSESSMENT IN OUTSOURCING

The Company shall identify, assess, monitor, and mitigate the risks associated with outsourcing of financial and non-financial services to ensure that outsourcing arrangements do not compromise its operational integrity, regulatory compliance, customer service, or business continuity.

Accordingly, the following categories of risks shall be evaluated prior to entering into, and throughout the lifecycle of, any outsourcing arrangement:

8.1. Strategic Risk: Risk that the service provider may act in a manner inconsistent with the strategic objectives and business goals of the Company, thereby adversely affecting long-term planning and positioning.

8.2. Reputation Risk: Risk arising from substandard service or conduct of the service provider which may impair customer confidence, damage the Company's brand image, or lead to negative publicity.

8.3. Compliance Risk: Risk that the service provider fails to comply with applicable regulatory, statutory, and legal requirements including those relating to data privacy, consumer protection, anti-money laundering, and KYC norms, thereby exposing the Company to enforcement actions or sanctions.

8.4. Operational Risk: Risk stemming from failure or disruption of systems, inadequate controls, fraud, human error, or financial incapacity of the service provider to fulfill contractual obligations or provide timely remedies.

8.5. Legal Risk: Risk of the Company becoming subject to legal liability, penalties, fines, or damages due to contractual breaches, negligence, misconduct, or non-compliance by the service provider.

8.6. Exit Strategy Risk: Risk arising from over-dependence on a single or limited number of service providers, erosion of in-house capabilities, or presence of contractual terms that inhibit timely disengagement or transition back in-house.

8.7. Counterparty Risk: Risk associated with inadequate due diligence or flawed credit assessment and underwriting

standards followed by the service provider, especially where third-party origination or processing is involved.

8.8. Contractual Risk: Risk that the Company is unable to enforce the terms and conditions of the outsourcing contract due to ambiguous provisions, lack of legal enforceability, or jurisdictional challenges.

8.9. Concentration and Systemic Risk: Risk arising when a significant portion of industry players or critical processes rely on a single or limited number of service providers, thereby limiting control and increasing vulnerability to systemic disruption.

8.10. Country Risk: Risk related to outsourcing to service providers located in foreign jurisdictions where political, legal, or social factors may pose additional threats to the continuity, legality, or security of outsourced services.

The Company shall ensure that all outsourcing arrangements, particularly those classified as material, are entered into after a thorough risk assessment and contain adequate clauses and safeguards to address these risks. Ongoing monitoring, audit, and reporting mechanisms shall be put in place to ensure continued oversight and compliance.

9. DUE-DILIGENCE OF SERVICE PROVIDER

9.1. Before entering into or renewing any outsourcing arrangement, the Company shall undertake comprehensive due diligence to evaluate the capability, integrity, and reliability of the proposed service provider. This due diligence process shall ensure that the service provider is fully equipped to meet the obligations stipulated under the outsourcing agreement and is compliant with the regulatory standards applicable to the Company.

9.2. While conducting due diligence prior to outsourcing any activity, the Company shall consider all applicable laws, regulations, guidelines,

and conditions imposed under its certificate of registration or any other approval or licensing by the RBI.

9.3. In line with governance standards, in case the service provider is not a group entity of the Company, it shall not be owned or controlled by any Director of the Company or their relatives, as defined under the Companies Act, 2013.

9.4. The due diligence shall be both qualitative and quantitative, encompassing financial, operational, technical, compliance, and reputational parameters, and shall specifically include an assessment of:

9.4.1. Proven track record and demonstrated capability to implement, manage, and support the proposed outsourced function effectively throughout the contracted period.

9.4.2. Evaluation of financial health, including liquidity position, net worth, and profitability, commensurate with the nature and criticality of the outsourced service, and the ability to sustain operations under adverse conditions.

9.4.3. Assessment of the service provider's market reputation, adherence to legal and regulatory obligations, historical track record of compliance, pendency of litigation, and record of complaints or disputes with other clients.

9.4.4. Adequacy of information security framework, internal control systems, audit mechanisms, reporting protocols, and monitoring arrangements, including safeguards to ensure employee integrity and prevent data misuse.

9.4.5. Robustness of the service provider's business continuity planning (BCP), disaster recovery capabilities, and ability to resume operations within acceptable timeframes in the event of disruptions.

9.4.6. Mechanisms in place for conducting background checks of employees and sub-service providers, ensuring appropriate

training and conduct standards, particularly where customer data and financial transactions are involved.

9.4.7. Compatibility of the service provider's systems and infrastructure with those of the Company, and adherence to expected levels of customer service, responsiveness, and quality benchmarks.

9.4.8. Assessment of whether the proposed outsourcing arrangement may lead to undue concentration with a single service provider, thereby increasing operational and dependency risk.

9.4.9. Wherever feasible, the Company shall supplement its own due diligence by obtaining third-party assessments, industry feedback, or independent reviews regarding the performance and credibility of the service provider.

9.5. All due diligence findings shall be documented by the company. The same shall be duly completed, reviewed by the respective Senior Management, and submitted to the Board as applicable, prior to final approval of the outsourcing arrangement.

10. OUTSOURCING AGREEMENT

10.1. *All outsourcing arrangements entered into by the Company shall be governed by a formal, written Outsourcing agreement* that clearly defines the rights, responsibilities, obligations, and liabilities of both the Company and the service provider.

10.2. The agreement shall be reviewed and vetted by the Company's legal counsel to ensure legal validity, enforceability, and alignment with applicable regulatory frameworks and risk mitigation principles.

10.3. The Agreement shall address the risks that may be incurred during the execution of the Contract and outline the appropriate risk mitigation strategies.

10.4. In the event of termination of a customer - dealing - service provider, the Company shall ensure mandatory public disclosure through branch notices, website posting, and direct customer communication. In circumstances where the customer is required to interact with

service providers, the Company shall make adequate disclosures in product literature, brochures, or other relevant documents like the Agreement, indicating the involvement of agents in the sale, marketing, or servicing of its products, with their roles outlined in broad terms.

10.5. The outsourcing agreement shall be comprehensive and sufficiently flexible to allow the Company to retain control over the outsourced functions and ensure compliance with legal, regulatory, and supervisory obligations. It shall explicitly define the legal nature of the relationship between the parties (e.g., principal-agent or otherwise) and address all relevant operational, financial, reputational, and legal risks.

10.6. Key provisions to be incorporated in every outsourcing agreement shall include, but not be limited to, the following:

Scope and Standards	Clearly define the outsourced activities, service levels, timelines, and performance metrics
Access Rights	Ensure full access to all relevant books, records, and data of the service provider
Monitoring	Allow for continuous performance review and the right to take corrective actions
Termination	Include a clear termination clause with notice period and grounds for termination, including convenience or breach
Confidentiality and Data Security	Impose strict obligations for maintaining data confidentiality and liability for breaches.
Business Continuity	Require robust business continuity and disaster recovery plans.
Subcontracting	Restrict subcontracting without prior written approval and ensure equivalent safeguards.
Audit Rights	Permit audits by the Company or its agents and access to audit reports

Regulatory Access	Allow RBI or its authorized representatives access to relevant records within reasonable time.
RBI Inspection	Recognize RBI's right to inspect the service provider's operations and records
Post-Termination Obligations	Mandate continued confidentiality and document retention even after contract termination.

11. INFORMATION SECURITY & CONFIDENTIALITY MEASURES

11.1. The Company shall take all necessary steps to preserve the security and confidentiality of customer information held by or accessible to the service provider, as public trust is critical to its stability and reputation.

11.2. Access to customer data by the service provider's personnel shall be strictly on a 'need-to-know' basis, limited to what is required to perform the outsourced function.

11.3. The service provider must ensure that the Company's customer information, records, and assets are securely segregated and identifiable, especially where the service provider services multiple entities, to prevent any comingling.

11.4. The Company shall regularly monitor and review the service provider's information security practices, requiring prompt disclosure of any security breaches.

11.5. Any breach or leakage of confidential customer information must be immediately reported to the RBI. The Company shall be liable to its customers for any resultant damages.

11.6. The service provider shall adopt industry best practices and regulatory standards for secure data handling, storage, transmission, and disposal. Customer data shall be stored only for as long as necessary and disposed of securely thereafter, in accordance with applicable laws and contractual obligations.

11.7. The Company shall ensure that the service provider and its employees, agents, and subcontractors sign appropriate Non-disclosure agreements (NDAs) to prevent unauthorized disclosure or misuse of customer data.

11.8. All customer data transmitted or accessed electronically by the service provider must be encrypted using strong, industry-standard encryption protocols to safeguard it from interception or tampering.

12. OBLIGATIONS OF DSA/DMA/RA

12.1. The Company shall ensure that the DSA/DMA/RA agents are adequately trained and equipped to carry out their responsibilities effectively and in compliance with the applicable guidelines.

12.2. The Company has a separate "*Code of Conduct for DSA/DMA/RA*" approved by the Board. All agents shall be required to provide a formal undertaking to adhere to this Code.

12.3. The Recovery Agents, if any, shall adhere to the Company's existing Fair Practice Code for the collection of dues and the repossession of security.

12.4. The Company and its agents shall strictly avoid any form of intimidation or harassment, whether verbal or physical, during debt collection. The acts include, but are not limited to, acts intended to humiliate publicly or impact the privacy of the debtor/his close ones, sending inappropriate messages either on mobile/social media, threatening or anonymous calls/messages, calling the borrower at inappropriate hours i.e. before 8:00 a.m. and after 7:00 p.m. for recovery of overdue loans or making false and misleading representations.

12.5. The service provider shall not, in any manner, obstruct or interfere with the Company's ability to monitor, supervise, or manage the outsourced activity. Further, such outsourcing shall not hamper or restrict the RBI in the performance of its supervisory and regulatory functions

13. SAFEGUARDS FOR OPERATIONAL CONTINUITY

13.1. The service provider shall be contractually obligated by the company to formulate, maintain, and periodically test its Business Continuity and Disaster Recovery Plan to ensure continuity of services under all circumstances. The Company may, at its discretion, conduct joint testing exercises with the service provider to verify operational readiness.

13.2. In order to safeguard against risks arising from the sudden termination of the outsourcing agreement or insolvency of the service provider, the Company shall retain effective control over the outsourced activities. The Company shall incorporate appropriate clauses in the outsourcing agreement to ensure that, in such events, it has the right to intervene and implement necessary measures to continue its operations and services without disruption. These provisions shall enable the Company to maintain business continuity and protect customer interests without incurring prohibitive expenses or operational interruptions.

13.3. The Company shall, as part of its contingency planning, assess the feasibility of identifying alternate service providers or reintegrating the outsourced function in-house. Such contingency assessments shall include considerations of cost, time, and resource implications to ensure timely execution during exigencies.

13.4. Where shared infrastructure, systems, or premises are used by the service provider, the Company shall ensure that its data, documents, records, and other assets are appropriately segregated and clearly identifiable. The service provider shall be contractually required to ensure that, in the event of contract termination or an emergency, such data and assets can be securely retrieved, deleted, destroyed, or rendered unusable to prevent misuse or unauthorized access.

13.5. The Company may conduct an annual review of the financial and operational condition of each service provider to evaluate their

continued ability to meet outsourcing obligations. This due diligence assessment be based on all relevant and available information and shall specifically identify any signs of deterioration in performance, breaches in confidentiality or data security, and weaknesses in business continuity preparedness. The findings of such reviews shall inform necessary corrective or mitigation measures to safeguard the Company's interests.

14. GRIEVANCE REDRESSAL IN OUTSOURCED ACTIVITIES

14.1. The Company has established a Grievance Redressal Mechanism in accordance with the guidelines prescribed by the RBI to address and resolve customer complaints, including those arising from services rendered by outsourced agencies.

14.2. At all operational locations, the Company shall prominently display the name, contact number (landline/mobile), and email address of the designated Grievance Redressal Officer. This officer shall be responsible for ensuring that all legitimate grievances are resolved promptly and effectively, without undue delay.

14.3. It shall be explicitly conveyed to customers that the Company's Grievance Redressal Mechanism covers issues related to services provided by third-party service providers and outsourced agencies.

14.4. The Company generally allows customers a period of 30 (thirty) days from the date of occurrence of the grievance to lodge their complaints. The grievance redressal procedure, along with the stipulated timelines for acknowledging, responding to, and resolving complaints, shall be clearly outlined and published on the Company's official website for public awareness and easy access.

15. INTRA - GROUP OUTSOURCING ARRANGEMENTS

15.1. The Company, while functioning within a group or conglomerate structure, may enter into outsourcing arrangements with group entities for certain support functions and services such as shared

premises, personnel, IT infrastructure, legal and professional services, centralized back-office operations, or financial services.

15.2. For such cases, the Company has formulated and shall adhere to the *Outsourcing within the Group Policy* which covers the principles and procedures for all the outsourcing arrangements with group entities to ensure effective governance, operational transparency, and compliance with applicable regulatory guidelines

16. OFF-SHORE OUTSOURCING OF FINANCIAL SERVICES

16.1. In instances where the Company engages service providers based outside India, the Company shall closely monitor relevant government policies and the political, social, economic, and legal environment.

16.2. The Company shall ensure that in case of off-shore outsourcing an appropriate contingency and exit strategies are structured by the company to deal with the country risk problems.

16.3. The Company shall only enter into arrangements with service providers situated in jurisdictions that generally uphold confidentiality clauses and agreements, and the governing law of the outsourcing contract shall be clearly specified.

16.4. In addition to the general outsourcing conditions, the following specific safeguards shall be adhered to while outsourcing financial services relating to Indian operations to offshore service providers:

16.4.1. Inspection: Where the offshore service provider is a regulated entity, the offshore regulator shall not obstruct the outsourcing arrangement or object to inspections by the Reserve Bank or visits by the Company's internal and external auditors.

16.4.2. Access to Record: Access to records by the Company's management and the Reserve Bank shall remain unaffected, even in the event of liquidation of either the offshore service provider or the Company in India.

16.4.3. Access to Data: The regulatory authority in the offshore location shall not access data related to the Indian operations of the Company solely due to processing being conducted offshore, except when the processing occurs in the Company's home country.

16.4.4. Jurisdiction: The jurisdiction of courts in the offshore location where data is maintained shall not extend to the Company's operations in India merely because the data is processed offshore.

16.4.5. Maintenance of Record: All original records shall continue to be maintained in India.

17. MAINTENANCE OF CENTRAL OUTSOURCING RECORDS

17.1. The Company shall maintain a centralised record of all material outsourcing arrangements in a manner that ensures it is readily accessible for review by the Board and senior management.

17.2. This central record shall be updated promptly upon execution, renewal, or termination of any outsourcing agreement.

17.3. A comprehensive review of the outsourcing arrangements, along with the updated record, shall be conducted on a half-yearly basis and placed before the Board/Risk Management Committee for their consideration and oversight.

18. AUDIT OF OUTSOURCING ARRANGEMENTS

18.1. The Internal Audit of the Company shall be conducted at periodic intervals by designated internal auditors. In instances where the internal auditors lack the requisite subject-matter expertise for specific areas, the Company may engage external professionals/Auditors on a contractual basis to assist in the audit process. However, such external assistance shall be limited to providing expert support, and the overall responsibility, control, and

ownership of the internal audit function shall remain with the Company's internal audit team and management.

18.2. The Company shall ensure that regular audits are undertaken to evaluate the effectiveness and adequacy of the risk management practices implemented in relation to its outsourcing arrangements and compliance with the applicable regulatory requirements, including those stipulated under relevant RBI guidelines.

18.3. The internal audit function of all outsourced activities shall also be put in place and monitored by the Audit Committee/Board of the company.

18.4. The Company shall ensure that, in cases where outsourced functions involve financial transactions such as cash management, comprehensive reconciliation of transactions is carried out in a timely and accurate manner between the Company, the service provider, and any sub-contractors engaged by the service provider. An ageing analysis of all unreconciled entries pending with outsourced vendors shall be prepared and presented periodically to the ACB. The Company shall take appropriate steps to resolve such outstanding items without undue delay and reduce long-pending items at the earliest.

19. REPORTING OF SUSPICIOUS TRANSACTIONS

19.1. The Company shall remain solely responsible for the submission of Currency Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) to the Financial Intelligence Unit-India (FIU-IND) or any other competent authority, in respect of customer-related activities undertaken by its service providers.

19.2. The outsourcing of such functions shall not dilute the Company's obligation to ensure full compliance with the applicable regulatory and statutory reporting requirements under the Prevention of Money Laundering Act (PMLA), 2002, and associated rules and guidelines.

20. APPROVAL, REVIEW & UPDATE

20.1. This Policy shall be approved by the Board and be reviewed periodically, at least on an annual basis, or as and when required, in response to changes in the regulatory framework, risk environment, or operational requirements.