Outsourcing Policy

(Version 4)

Name	Policy on Outsourcing of services
Owner of the document	Chief Financial Officer Chief Data and Operations Officer Chief Regulatory Officer Chief Technology Officer Chief Risk Officer Chief of Business Development, New Projects and DP Training

Table of Content:

1. Introduction

1.1 In an ever-evolving landscape of financial services, Central Depository Services (India) Limited (CDSL), recognises the strategic importance of outsourcing in optimising operational efficiency and maintaining a competitive edge.

1.2 This Outsourcing policy serves as a guiding framework to ensure that our outsourcing activities are aligned with regulatory standards, risk management practices, and the overarching goal of delivering reliable and secure services to our clients.

1.3 This document shall be read in conjunction with the following documents:

i. SEBI Circular no. CIR/MRD/DP/19/2015 on Outsourcing by Depositories
ii. SEBI (Depositories and Participants) Regulations, 2018
iii. CDSL Procurement Policy
iv. Circulars issued by SEBI from time to time.

1.4 This policy shall not be applicable for Goods/ Services Procurement contracts.

2. Terms and Definition

2.1 Outsourcing – Outsourcing may be defined as the use of one or more than one, 3rd party – either within or outside the group to perform the activities associated with services which are offered.

2.2 Procurement – Acquisition by purchase, lease or other legal means of the goods, services, job-works, and consumables in a nature of either capital or revenue expenses, used by CDSL to discharge its functions in an effective, efficient and economic manner.

2.3 Source Department – It is the Department which has outsourced or is in the process of outsourcing any activity for which they are responsible.

2.4 Outsourced Entity – It is the third party engaged by Source Department for outsourcing any activity for which the Source Department is responsible.

2.5 Designated Point of Contact(s) – The Designated Point of Contact(s) (POC) appointed by the Source Department shall ensure compliance with the principles outlined in the Outsourcing Policy and shall be responsible for coordinating all activities related to outsourcing contracts.

3. Scope and exceptions

3.1 All Outsourcing shall be done in adherence with this policy and the outsourcing shall be done by the officers in conformity with financial delegation.

3.2 In exceptional circumstances or exigencies, requirement of policy can be waived by the MD & CEO. In case the MD & CEO is not available then the Board of Directors can waive the requirements of the policy. The reasons for such a waiver should be documented properly.

4. Objective

4.1 Key objectives of this policy are to:

i. Establish a clear and structured vendor selection procedure incorporating due diligence and risk impact analysis for informed decision making.

ii. Ensure adherence to regulatory requirements in all outsourcing activities maintaining industry standards and legal obligations.

iii. Ensure that checks and balances outlined in this policy are observed whenever any activity is outsourced.

iv. Implement robust contingency plans, periodic audits and confidentiality measures to mitigate risks and protect sensitive information.

v. Ensure that core activities as specified in the SEBI Circular are not outsourced.

vi. Regularly review the Outsourcing policy to adapt to evolving industry dynamics

5. Activities that cannot be outsourced

5.1 CDSL as a depository shall not outsource its following core activities:

i. Processing of the applications for admission of Depository Participants (DPs), Issuers and Registrar & Transfer Agents (RTAs). However, the function of storing of related documents and records may be outsourced to a reputed vendor specializing in this line of business.

ii. Facilitating Issuers/RTAs to execute Corporate Actions. However, documents/records relating to corporate actions may be stored with a reputed vendor specializing in this line of business.

iii. Allotting ISINs for security.

iv. Maintenance and safekeeping of Beneficial Owner's data.

v. Execution of settlement and other incidental activities for pay-in/ pay-out of securities.

vi. Execution of transfer of securities and other transactions like pledge, freeze, etc.

vii. Provision of internet-based facilities for access to demat accounts and submitting delivery instructions.

viii. Ensuring continuous connectivity to DPs, RTAs, Clearing Corporations, and other Depository. However, CDSL would facilitate its DPs, RTAs, Clearing Corporations, and other Depository to obtain connectivity from the service providers and will not deactivate any DP or RTA except when in case of termination, after following due process of termination.

ix. Monitoring and redressal of investor grievances.

x. Inspection of DPs and RTAs. However, the activity of making entry of Audit/Inspection Reports received from the DPs in CDSL back-office system i.e. maker level activity may be outsourced who will perform the job under the supervision of employees of CDSL.

xi. Surveillance Functions.

xii. Compliance Functions.

5.2 Further core activities of Information Technology should not be outsourced to the extent possible. Maintenance of depository system may be outsourced to a vendor of repute whose work will be tested by the in-house CDSL team before release. Peripheral software development and maintenance may be outsourced after following due diligence guidelines. Hardware, if taken on lease, from a reputed vendor, will be housed in CDSL premises with AMC arrangements.

6. Vendor Selection Procedure

6.1 CDSL shall prepare a list of potential vendors for outsourcing. The tender form / specification requirement should be communicated to vendors. The number of potential vendors is to be decided by the Source Department. A minimum of two (2) quotations should normally be invited for outsourcing up to Rs.1,00,000/- per instance per vendor exclusive of taxes and three (3) quotations should be invited for outsourcing in excess of Rs.1,00,000/- per instance per vendor exclusive of taxes

6.2 The validity of all quotations provided by vendors shall be for a period of 12 months from the date of receipt of the quotation.

6.3 In certain circumstances, exceptions may be made to the quotation invitation process. Some examples of the exceptions may include engaging with exclusive suppliers, vendors with specific expertise, etc. In such cases, a detailed justification should be placed on record.

6.4 Notwithstanding the 12-month validity period of quotations, fresh quotations may be invited under the following circumstances:

i. If there is a reduction in the contracted rate as specified in the contract.
ii. If, at the time of renewing or extending the outsourcing activity, the prevailing exchange rate (where applicable) is more favourable than the rate initially agreed upon in the contract.

6.5 Below is the indicative list of vendor selection criteria:

i. Reputation, experience and clientele
ii. Resources capabilities, expertise and skills
iii. Change, adaptability, and project management experience
iv. Flexibility and innovative
v. Quality and Cost advantage
vi. Timelines / Lead time of the vendor

6.6 Annexure 1 defines the minimum standards/thresholds in terms of quantitative and qualitative parameters for the above indicative list of vendor selection criteria. Any additional criteria which are more relevant, keeping in mind the nature of activities, may be considered.

6.7 Preference shall be given to the vendors offering all the required services under one roof and having a range of qualities related to the services offered.

6.8 There should not be conflict of interest in the process of selection of Vendor.

6.9 Vendor selection emphasis should not be limited to services, technical and commercial evaluations but also focus on addressing issues like technical and process trainings, testing, organisational change activities, customisation, updates, and maintenance etc.

6.10 In addition, for outsourcing contracts, due diligence process will be conducted by the Source Department. For details on the due diligence process please refer to Section 8.

7. Outsourcing of Large Projects

7.1 The vendor selection process for large project should be in line with the guidelines laid down in the large project RFP management documents, attached in the updated Procurement Policy

7.2 Final recommendations will be placed before the CDSL Audit Committee and on their recommendation to the CDSL Board for approval.

8. Due Diligence

8.1 The Company shall conduct appropriate due diligence in selecting the third party to whom activity is proposed to be outsourced and ensure that only reputed entities having proven high delivery standards are selected.

8.2 The Source Department shall conduct due diligence/enhanced due diligence of the third-party during vendor selection. The process for diligence/enhanced due diligence is described in detail in this section.

8.3 The process of due diligence is dependent on the materiality of the outsourcing arrangement which will be determined on the basis of below inclusive factors:

i. The impact of failure of a third party to adequately perform the activity on the financial, reputational and operational performance of the company and on the investors / clients.

ii. Ability of the Company to cope up with the work, in case of non-performance or failure by a third party by having suitable back-up arrangements.

iii. Regulatory status of the third party, including its fitness and probity status.

iv. Other factors such as financial impact, strategic importance, operational significance, regulatory requirements, customer impact and cost & efficiency.

These criteria ensure that a risk based due diligence is conducted and appropriate assessment of outsourcing arrangements that pose significant risks or have substantial impact on the CDSL's operations is conducted.

8.4 Material Outsourcing arrangements shall go through enhanced due diligence (in addition to normal due diligence) and other outsourcing arrangements shall be subjected only to the normal due diligence process.

8.5 Due diligence shall include, among other things, an assessment of the below factors:

i. Third-party's resources and capabilities, including financial soundness, to perform the outsourcing work within the fixed timelines.
ii. Compatibility of the practices and systems of the third party with the company's requirements and objectives.
iii. Market feedback on the prospective third party's business reputation and track record of their services rendered in the past.
iv. Level of concentration of the outsourced arrangements with a single third party.
v. The environment of the foreign country where the third party is located, if applicable

8.6 In addition to the factors mentioned in clause 8.5, the below mentioned factors may be considered while performing Enhanced Due Diligence:

i. Review of past/ongoing legal proceedings against the third party.
ii. Review of third party's Data Protection policies and compliance with the data privacy laws.
iii. Review of third party's Incident response and recovery plan.
iv. Evaluate the third party's cybersecurity measures and protocols.
v. Review of third party's Code of conduct and ethical guidelines, Anti-bribery & corruption policies and Corporate Governance practices.
vi. Inspection of third party's premises (wherever required).
vii. Review of third party's track record for continuous improvement and learning.

8.7 Due care should be exercised while outsourcing multiple activities to the same entity, as over-reliance may pose concentration risks.

9. Risk Impact Analysis

9.1 Outsourcing an activity inherently introduces Outsourcing risk. A comprehensive Risk Impact Analysis is crucial in assessing and understanding the potential risks associated with engaging Outsourced entity.

9.2 Risk impact analysis to be done before outsourcing any activity and appropriate risk mitigation measures like back up/ restoration system should be in place.

9.3 A systematic approach allows an organization to anticipate, evaluate and effectively mitigate risks, ensuring a resilient and well-informed outsourcing strategy.

9.4 The Risk Management Department shall perform risk assessment for new outsourcing arrangements.

9.5 The following list of indicative risks may be considered, among others, while performing a risk impact analysis.

i. Operational risk
ii. Financial risk
iii. Compliance and Legal risk
iv. Cyber Security risk
v. Reputational risk
vi. Contractual risk
vii. Technological risk
viii. Project Management risk
ix. Human Resource risk

9.6 Please refer to Annexure 2 for key risk mitigation strategies related to the risks mentioned above:

9.7 The Department outsourcing its activities shall be responsible for submitting all the necessary information and documentation to the Risk Management Department for the risk assessment prior to outsourcing the activity.

9.8 After conducting the risk analysis on the outsourced activities, the findings and recommendations will be communicated to the Source Department. If any risks are identified which require implementing controls/mitigation plan for the same, the

Risk Management Department, in consultation with the Source Department must promptly address them by developing appropriate risk strategies like mitigation, transfer, acceptance, and termination.

9.9 The Risk Impact Analysis for all the existing outsourcing arrangements shall be performed on a periodic basis.

9.10 A report on due diligence and risk impact analysis shall form part of the approval documents.

10. Outsourcing Agreement

10.1 Outsourcing relationships shall be governed by written contract arrangements/ terms and conditions that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of the parties to the contract, termination procedures. A separate confidentiality/ non-disclosure agreement shall be entered into with the counterparty prior to any outsourcing of activities.

10.2 Care should be taken to ensure that the below mentioned indicative list is considered while drafting the Outsourcing Contract:

i. Clearly defines what activities are going to be outsourced, including appropriate service and performance levels.

ii. Provides for mutual rights, obligations and responsibilities of CDSL and the third party, including indemnity by the parties.

iii. Provides for the liability of the third party to CDSL for unsatisfactory performance/other breach of the contract.

iv. Provides for the continuous monitoring and assessment by CDSL of the third party so that any necessary corrective measures can be taken up immediately, i.e., the contract shall enable CDSL to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet legal and regulatory obligations.

v. Includes, where necessary, conditions of sub-contracting by the third-party, i.e. the contract shall enable CDSL to maintain a similar control over the risks when a third party outsources to further third parties as in the original direct outsourcing.

vi. Has unambiguous confidentiality clauses to ensure protection of proprietary and customer data during the tenure of the contract and also after the expiry of the contract.

vii. Specifies the responsibilities of the third party with respect to the IT security and contingency plans, insurance cover, business continuity and disaster recovery plans, force majeure clause, etc.

viii. Provides for preservation of the documents and data by third party.

ix. Provides for the mechanisms to resolve disputes arising from implementation of the outsourcing contract.

x. Provides for termination of the contract, termination rights, transfer of information and exit strategies.

xi. Addresses additional issues arising from country risks and potential obstacles in exercising oversight and management of the arrangements when CDSL outsources its activities to foreign third party. (For example, the contract shall include choice-of-law provisions and agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction)

xii. Neither prevents nor impedes CDSL from meeting its respective regulatory obligations, nor the regulator from exercising its regulatory powers.

xiii. Provides for CDSL and /or the regulator or the persons authorized by it to have the ability to inspect, access all books, records and information relevant to the outsourced activity with the third party

xiv. Provides for the period of contract, deliverables, timelines, applicable taxes and terms of payment.

xv. Provides for the responsibility of placing appropriate safeguards for ensuring data security and confidentiality and ensuring that there is no co-mingling of information.

xvi. Provides for renegotiation and renewal of contract.

xvii. Provides for non-poaching of employees.

11. Approvals, Invoicing etc.

For Guidelines on Approvals and Invoicing, refer to guidelines given in the updated Procurement Policy.

12. Roles and Responsibilities of Source Department

12.1 The Source Department shall preserve and regularly update records relating to all activities outsourced so that the same is readily accessible for review by the Board of Directors and / or senior management, as and when needed.

12.2 The Source Department shall be responsible for monitoring the performance of Outsourced entity, undertaking periodic tests of the critical systems & security procedures and review of their backup facilities so that any necessary corrective measures can be taken up immediately.

12.3 The Source Department may be permitted to further sub-contract the activities only when the Outsourced entity has entered into back-to-back agreement with the third-party and ensuring that appropriate due diligence is conducted for such third-party.

12.4 The Source Department shall designate a Point of Contact(s) (POC) who will ensure adherence to the principles outlined in the Outsourcing Policy. The Designated POC will be responsible for coordinating all activities related to outsourcing contracts.

13. Renewal Process

13.1 In cases of renewal, a review should be conducted, based on the services rendered, cost benefit analysis of the market trends, regulatory requirements etc.

13.2 The terms of the agreements shall also be reviewed at the time of renewal and placed for approval by the respective Departments, as per the approved Delegation of Power. Additionally, the performance of vendors and Service Level Agreements (SLA), wherever applicable, should be monitored by the respective Departments and recorded in the approval note.

14. Contingency Plan

14.1 Vendor shall have Business Continuity and Disaster Recovery Plan in place so as to ensure uninterrupted service to CDSL and for taking care of contingencies.

14.2 Vendors should be made aware of CDSL's Recovery Time Objective

15. Audit

15.1 The Department which proposes to outsource any activity should describe in the memorandum detailed task to be outsourced to a vendor, so that the memorandum acts as a basis / reference point for audit of activities.

16. Caveat

16.1 No outsourcing arrangement should impair the ability of CDSL / Auditor /Regulator to exercise its responsibility of supervision/inspection.

17. Review of Outsourcing Policy

17.1 This policy shall be reviewed periodically to ensure that it remains appropriate, in light of the changing business environment, and to ensure that such principles and policies are effectively implemented.

17.2 The policy shall be reviewed at least once in 3 (three) financial years for effective implementation with the approval of appropriate authority / Committee.

Review Frequency: Once in Three Financial Years

Last Reviewed on: October 2024

Document Control:

Version	Author	Reviewer	Approved by	Date
Version-1	Legal & Secretarial Department	SVP & Group Company Secretary	Board of Directors	January 2016
Version-2	Legal & Secretarial Department	AZB & Partners	Board of Directors	October 2017
Version-3	1. Chief Financial Officer 2. Chief Data & Operations Officer 3. Chief Regulatory Officer 4. Chief Technology Officer 5. Chief Risk Officer 6. Chief of Business Development, New Projects and DP Training	Audit Committee	Board of Directors	October 2024
Version-4	1. Chief Financial Officer 2. Chief Data & Operations Officer 3. Chief Regulatory Officer 4. Chief Technology Officer 5. Chief Risk Officer 6. Chief of Business Development, New Projects and DP Training	Audit Committee	Board of Directors	March 2025

ANNEXURE 1 - Minimum standards/thresholds in terms of quantitative and qualitative parameters

1. Quantitative Parameters:

Criteria	Minimum standards/thresholds
Financial Soundness	• The third-party's financial stability and capability to perform the outsourcing work within the fixed timelines
Resources and Capabilities	• Adequate resources, expertise, and skills to meet the company's requirements
Market Reputation	• Positive market feedback and a proven track record of services rendered in the past
Compliance with Regulations	• Adherence to regulatory requirements and fitness and probity status

2. Qualitative Parameters:

Criteria	Minimum standards/thresholds
Compatibility	• Compatibility of the third-party's practices and systems with the company's requirements and objectives
Confidentiality:	• Unambiguous confidentiality clauses to ensure the protection of proprietary and customer data during and after the contract
Business Continuity and Disaster Recovery	• The vendor must have a Business Continuity and Disaster Recovery Plan in place to ensure uninterrupted service
Cybersecurity Measures	• Evaluation of the third-party's cybersecurity measures and protocols
Ethical Guidelines	• Review of the third-party's code of conduct, anti-bribery and corruption policies, and corporate governance practices

ANNEXURE 2 - Key risk mitigation strategies

Sr. No.	Risk	Key Risk mitigation strategies
1	Operational Risk	• Conduct assessments before onboarding and conduct periodic assessments. • Existence of Business Continuity and Disaster Recovery Plan
2	Financial & Credit Risk	• Conduct financial assessments
3	Cybersecurity & Data Security Risk	• Verify regulatory certifications and track record in handling critical operations. • Conduct periodic security audits • Mandate incident reporting as per regulatory requirements. • Require geographically diverse disaster recovery (DR) sites. • Ensure secured data transfer • Enforce non-disclosure agreement
4	Legal & Regulatory Compliance Risk	• Incorporate relevant contractual clauses as needed; see Section 10.2 of this document for reference. • Annual compliance audits and enforce mandatory regulatory reporting.
5	Reputational Risk	• Include indemnity provisions in contract
6	Technological Risk	• Periodic assessments and audits. • Compliance with industry-standard tech frameworks. • Redundancy measures for critical IT infrastructure.
7	Project Management Risk	• Defined milestones and KPIs for projects. • Periodic progress reviews with vendor accountability measures. • Implementing SLA monitoring • Contractual penalties for missed deadlines
8	Human Resource Risk	• Minimum skill and experience criteria for vendor personnel. • Knowledge transfer plans • Annual training and upskilling requirements • Background verification as may be required
9	Concentration & Dependency Risk	• Avoid reliance on a single vendor for mission-critical functions • Explore options for backup vendors as needed.