Vendor Management and Outsourcing Policy

A.TREDS Limited

October 2025

Document Control Sheet

Version Control & review

Version	Month/Year	Change Description
5	October 2025	Aligned with the group policy and RBI outsourcing guidelines

Description	Name	Designation	Date
Changes Suggested by	Meenakshi Agarwal	Company Secretary & Compliance Officer	23.09.2025
Reviewed By	Prakash Sankaran	MD&CEO	04.10.2025
Put up to Risk Management Committee of the Board for review	N.A.	N.A.	10.10.2025
Put up to The Board for approval	N.A.	N.A.	10.10.2025
Document maintained by	Audit and Risk team		

Table of Contents

I. Introduction 4
a. Definition 4
b. Objective 4
II. Ethical Considerations 4
III. Cost Benefit analysis 5
IV. Requisition for products and services 5
V. Activities not to be outsourced 6
VI. Vendor Identification and Empanelment Criteria 7
VII. Vendor Onboarding 8
VIII. Release of Purchase Order / Contractual requirements 9
IX. Vendor Management 10
a. Record Management 10
b. Reporting to Board/RMC/ORMC 10
X. Vendor Performance Evaluation 11
XI. Vendor suspension/ discontinuation/ blacklisting 11
XII. Vendor Bill Processing 12
XIII. Vendor Risk Management Audit 13
XIV. Vendor Business Continuity Plan 13
XV. Vendor Client Interaction and Redressal of Grievances relating to Outsourced services 14
XVI. Sub-Contracting 15
XVII. Role of the Board/Risk Management Committee/Audit Committee of the Board 15
XVIII. Ultimate Responsibility & Accountability 15
XIX. Review and Exceptions 16
1. Procedure for Product / Service Requisition & Vendor Identification 17
2. Procedure for Vendor Suspension / Termination 19
Annexure 2: Vendor/Service Provider Verification/Assessment Report 23
Annexure 3 : Template for Review of Service Provider/vendor 27

I. Introduction

a. Definition

'Outsourcing' may be defined as A.TREDS Limited's (ATL) use of a third party (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 ATL itself, now or in the future. 'Continuing basis' would include agreements for a limited period. Outsourcing in PSOs is governed by guidelines issued by RBI from time to time (Framework for Outsourcing of Payment and Settlement-related Activities by Payment System Operators- RBI circular CO.DPSS.POLC.No.S-384/02.32.001/2021-2022 dated August 3, 2021)

This policy formalizes the vendor management and outsourcing rules and associated processes for ATL. Vendors or service providers of ATL may include outsourced agents of ATL that act on behalf of ATL as partners/ joint ventures, product or service providers, and contracting counterparties for specific assignments, including, but not limited to software development, testing, etc.

b. Objective

The overall objective of this Policy is to procure quality products and services in the most cost-effective manner and satisfy the Company's requirements on a timely basis, consistent with Company's objective while maintaining the highest ethical standards. Functional departments shall be responsible for the procurement for their department specific products and services ("Procurer"). These respective departments shall aim to acquire quality products and services in a cost-effective manner. The procurer after finalizing the vendor shall seek approval from the CFO from cost and provision perspective and final sign off authority shall be as per delegation matrix mentioned in this policy (except ongoing expenses i.e. repair, maintenance, etc. where department head is the final authority).

In support of this objective, Procurer along with guidance of Common Procurer (CPT) of the group (if required) will:

- Resolve queries and complaints on all purchased products and services
- Ensure relevant information is gathered on market conditions, trends, prices, government regulations, etc.
- Follow defined procedures for procurement
- Raise Request for Proposal (RFP), wherever it is required

II. Ethical Considerations

ATL's procurement activities are conducted with complete impartiality and with no preferential treatment. ATLs Employees will not solicit or accept, directly or indirectly, any gratuity, gift, favor, entertainment, loan, or anything of monetary value from anyone who: (a) has or is seeking to obtain business; or (b) has interests that may be substantially affected by a procurement award. ATL vendors and their employees are expected to abide by the highest ethical, legal and moral standards in all business relationships. As such, all vendors are obliged to respect the company's policy and refrain from placing Employee in an ethical dilemma by offering entertainment, hospitality or gifts.

A Conflict of Interest is a situation where one or more persons or entities have controlled interests, and the serving of interest may be detrimental to another when an activity is being carried out by a third party.

As per RBI guidelines on Outsourcing, the service provider if it is not a group company of the PSO should not be owned or controlled by any director or officer/employee of PSO or their relatives having the same meaning as assigned under Companies Act, 2013. A Vendor Declaration on Conflict of Interest in this regard needs to be obtained while sending the vendor form for approval -"None of the ATL employees involved in the evaluation, selection or approval process shall have any interest, either directly or indirectly in the empanelment of any of the shortlisted vendors"

III. Cost Benefit analysis

Cost Benefit analysis shall be done and documented in connection with every procurement action above INR 50,000 in value. Price analysis may be accomplished in various ways, including the comparison of price quotations submitted, market prices and similar guidelines, together with discounts.

Exception: Annual Maintenance Contract pertaining to fixed assets and recurring services, commodity hardware / software (for eg.: laptops, MS 365 License, etc), pre-approved rate contracts.

IV. Requisition for products and services

Department to draft their procurement requisition mentioning the product/service specifications, required quantity, delivery timeline and delivery location. For R&R, Gifts and Events related procurements, the product/service requisition form should be filled and shared by Administration team once requisite internal approvals have been obtained.

All IT related procurements should be done by IT team and all non-IT related procurements should be done by Administration team. Any department specific procurement will be handled by the department themselves.

- ☐ Types of IT Products and Services procured
  - ☐ Softwares
  - ☐ Servers
  - ☐ Switches
  - ☐ Subscription Licenses
  - ☐ Data Centre equipments
  - ☐ Media Tapes
  - ☐ Operating System Licenses
  - ☐ Purchase of assets like Computers, Laptops
  - ☐ Annual Maintenance Contract (AMC) for assets like Computers, Laptops
  - ☐ Services AMC for resources
  - ☐ Service packages for application development & Maintenance

- Others as per requirement

- Types of Non-IT Products & Services taken from Vendors
  - Security and House Keeping Services
  - Purchase of assets like Air conditioners, Television, telephone sets, microwave, crockery etc.
  - Annual Maintenance Contract (AMC) for assets like Air Conditioners etc.
  - Car Rental Services
  - Travel Services by Air / Rail / Bus and Hotel booking
  - Civil / Electrical / Carpentry Maintenance
  - Storage of Documents
  - Telephone & lease lines
  - Data cards & SIM Cards
  - Procurement of Corporate items, R&R & Gifts
  - Organizing Events
  - Other goods & services as per requirement

V. Activities not to be outsourced

ATL can't outsource core management functions including risk management and internal audit; compliance and decision-making functions such as determining compliance with KYC norms. However, while internal audit function itself is a management process, the auditors for this purpose can be appointed by ATL from its own employees or from the outside on contract.

Core management function include:

- Internal audit functions
- Compliance functions
- Decision-making functions like determining compliance with KYC norms for opening customer accounts
- Management of Payment System operations
- Transaction management
- According sanction to merchants for acquiring, managing customer data
- Risk Management
- Information Technology & Information security management[1]

[1] While Information security tools for activities like VA-PT, Appsec, SOC, etc are outsourced to vendor, the management of the same resides with ATL

VI. Vendor Identification and Empanelment Criteria

Relevant departments based on product & service requisitions, shall identify Vendors. Identified vendors must meet the ATLs requirement related to product, service quality, delivery systems, price, and service objectives.

Some of the important vendors attributes, ATL may consider in vendor selection are as follows:-

a) Performance history
b) Facilities and Technical strength
c) Financial status
d) Organization and Management
e) Reputation
f) Systems
g) Procedural compliance
h) Labor relations
i) Environmental performance
j) IT Security measures
k) Site Visit
l) Existing customers
m) Business Continuity Planning
n) Diversity achievements and location

Prior to considering any outsourcing service provider, due diligence shall be performed that includes, but is not limited to the following aspects for evaluating the capability of service provider:

a. Past experience and competence to implement and support the proposed activity over the contracted period
b. Financial soundness and ability to service commitments even under adverse conditions
c. Business reputation and culture, compliance, complaints and outstanding or potential litigation
d. Security and internal control, audit coverage, reporting and monitoring environment, business continuity management
e. Ensuring due diligence by service provider of its employees
f. Compliance of relevant laws, regulations, guidelines and conditions of approval, licensing or registration
g. Name screening checks
h. All information and cyber security controls in line with the RBI requirements and adhere to ATL's laid out information and cyber security policies, standards related to scope of services. Outsourcing vendor to be evaluated as per the integrated vendor risk assessment framework for on-boarding assessment, as applicable
i. The service provider, if not a group company of Axis Bank, will not be owned or controlled by any director or officer/employee of Axis Bank or their relatives as defined in the latest Companies act.
j. Conflict with any of the other activities being delivered by the service provider to ATL.

k. The vendor must have the relevant infrastructure including manpower, experience etc. of providing similar services of at least two years.

Outsourcing within a group/conglomerate

The RBI Guidelines on outsourcing will be followed for arrangements with group entities, and all the requirements would be same that would be followed for any external vendor as stated in this Policy.

VII. Vendor Onboarding

Procurer will prepare the Cost Benefit analysis note (where applicable) along with the price quotations from selected vendors who meet the defined criteria; and present it to MD&CEO for his review. Minimum three quotations shall be obtained from three different vendors for the required product / service. If a pre-approved rate contract (either with the group company or with ATL) exists and is valid, then multi-vendor evaluation is optional. Any exceptions in the above process to be put up to MD & CEO for waiver, with proper justification. It is the responsibility of the respective user department to finalize the various terms and conditions with vendor in terms of delivery pattern & timeline, payment terms, scope of work etc. after which it may be sent to the CPT for further due diligence and negotiation (Respective Department Head to decide).

Central Procurer of Group (CPT)

Benefits of CPT of Group:

- Travel / Hotel desk are already integrated with Group Travel Desk
- CPT's catalogue and vendor wise rate cards for CAPEX and OPEX items are provided by CPT team. The Company can use this CPT rate card for all its requirements.
- The CPT process will bring in efficiency & Cost Control.
- The Company can utilize scale benefits in common areas and Shared Infrastructure.
- This will also lead to avoidance of duplication of efforts and will lead to effective cost control.

Role of Group CPT

- ATL will decide their requirements, specifications, vendors, and commercial terms as per their business needs and policies.
- CPT may work with vendors to make them agree and extend commercials terms finalized for the Group with ATL.
- Participate in requested meetings to support ATL with necessary knowledge / information.
- Share best practices for vendor management with ATL.
- Group's CPT shall be assisting and consulting ATL in case of requirement. However, all decision making and ownership shall rest with ATL and the process of vendor selection and procurement shall be followed as mentioned in this policy.
- ATL can take all procurement decisions themselves, irrespective of the amount and reach out to Group CPT only when they require help and assistance
- CPT will share details, if a vendor has been blacklisted by them, basis which ATL can take an independent call whether or not to continue with the vendor services

Other considerations

The first level of approval of outsourcing of existing/new process will be given by Department Head for their relevant vendors. The existing process of approving a product/ process where outsourcing is envisaged will happen after the approval of outsourcing of the process is taken from MD&CEO. All procurements shall be approved as per delegation matrix.

Once the vendor gets approved by concerned authorities, the Vendor should submit necessary documents. The vendor may have to produce original documents for verification, as and when called for by ATL. It is the responsibility of the Procurer to submit the details of the vendor for registering them. At the same time Procurer should share the supporting documents submitted by the vendor to Legal team for initiating the Contract or Service Level Agreement with concerned vendor, for their respective procurements.

Vendor should be registered on the execution of Contract or Service Level Agreement by:

- Administration team / Procurer for supply of non-IT product / service
- IT team for the supply of IT product / service
- F&A team for bill payment
- Legal team for monitoring contractual obligations and renewal of agreement

Vendors to be graded in terms of criticality of outsourcing:

a. **Critical Vendors**, are categorised from two perspectives:
   - Information Security perspective that would include cases where the A.TReDS network extends to vendor or the vendor has onsite access to A.TReDS network and where high volumes of aggregated Sensitive Personal data or information (SPDI) and Personal identifiable Information (PII) are shared with the vendor, and/or;
   - Where there is dependence on outsourced service provider's proprietary software/IT System/Application Services and there is no backup of alternate vendor availability.

b. **Non-Critical Vendors**, are all vendors not falling under the above criteria and where no SPDI / PII is shared with the vendor and where the vendor doesn't have direct network connectivity to A.TReDS.

VIII. Release of Purchase Order / Contractual requirements

Departments should ensure that a written agreement is executed with the vendor in the service provider agreement provided by legal, prior to on-boarding of the Service Provider.

- The department should ensure timely renewal of agreement and that the services of the vendor are availed only with valid agreement in place.
- The agreement should also bring out the nature of legal relationship between the parties- i.e. whether agent, principal or otherwise.
- Every outsourcing agreement should address the risks and risk mitigation strategies.
- Departments shall ensure that the service provider Agreement format as circulated by legal, as may be amended or modified from time to time, is being used while executing the agreement with the vendor. Deviations if any in the service provider Agreement, needs to be approved by the legal
- Renewal of outsourcing agreements should be initiated prior to expiry to avoid any business impact.

- In case of one time procurement/Service in the nature of corporate gifting, application procurement, etc., signing of Agreement is not mandatory, instead PO should contain the terms of procurement/service.

On execution of Contract / Service Level Agreement with the concerned vendor, the Central Administration team / Procurer & IT team shall release Purchase order or Letter of Intent to vendor for their respective procurements.

Any deviation should have a prior approval from Legal team.

IX. Vendor Management

Vendors must meet the ATL requirements related to product / service quality, delivery timelines, price, and service objectives. This would involve maintaining up-to-date records pertaining to vendors, carrying out periodic performance review of vendors and timely processing of bills received from vendors.

a. Record Management

i. Administration team should maintain an up-to-date Vendor master list for all vendors supplying non-IT products and services.

ii. Similarly, IT team should maintain an up-to-date Vendor master list for all vendors supplying IT products and services.

iii. For any other department specific vendor, list shall be maintained by the respective department

iv. Legal team shall be the custodian of all products / service contracts or SLA executed along with supporting documents. They shall also be responsible for tracking the contract expiry and sending reminders to Procurer regarding contract renewal for their concerned vendors.

v. Finance & Accounts team should maintain an up-to-date vendor master list for all registered vendors for bill processing and payment purpose.

vi. Any addition or removal from list of vendors shall be immediately intimated to the Risk team along with F&A.

b. Reporting to Board/RMC/ORMC

A central record of all outsourcing arrangements is available. Specifically, critical outsourcing is readily accessible for review by the RMC/Board. The records will be updated promptly and half yearly reviews will be placed before the Senior Management in Operational Risk Management Committee (ORMC) and/or Risk Management Committee of the Board.

X. Vendor Performance Evaluation

Periodic evaluation of vendor performance shall be carried out by Procurer for respective vendors either solely or jointly with concerned departments. Performance evaluation can be done on pre-defined parameters for example:

- Product / Service Delivery
- Replacement of damaged products
- Following the instructions given
- Prompt servicing of adhoc or urgent requirements
- Operational efficiency

Performance evaluation can be done using the following wherever possible:

- Using data from system or manual trackers maintained
- Periodic site visits wherever possible
- Periodic product / service quality check
- Obtaining feedback from end users

There shall be half yearly review for all critical vendors. Any deviation in the performance should be notified to vendor for immediate corrective action. Follow-up should be done with vendor for ensuring preventive measures have been implemented to avoid reoccurrence of similar deviation. Any contractual deviation should be brought to the notice of Legal team for taking appropriate action.

Financial penalties and liabilities may be imposed on the vendors on account of:

i. Inadequate availability of services related to downtime, unavailability of alternative service channels etc.
ii. Quality of services including performance guarantee, no. of defects in a particular software, gaps in the processes, delay in services.

Penalty may include:-

- Financial Penalty: Vendor to pay back ATL a portion of the damages or service failure as agreed by both the parties.
- Service Credits: When the agreed level of service is not maintained, vendor to offer credit to ATL for duration as mentioned in SLA.
- Extension of License or support: If an SLA is dishonored, the vendor has to extend the term of the license or support provided to the customer.

XI. Vendor suspension/ discontinuation/ blacklisting

Based on assessment and recommendation of the user department, contract with the vendor may be suspended / terminated on account of:

- Prolonged poor performance and agreed performance standards, as decided by user department

- Instance of fraud/ money laundering/ corruption/ bribery
- Leakage of information/data
- Breach of client's confidential data
- Vendor risks that are beyond the risk appetite of the company
- Bad market reputation of the vendor
- Involvement in unlawful and illegal activities
- Blacklisted by any regulator (IBA, SEBI, RBI, GOI, or any other regulator)
- Any other compelling reason which is detrimental to ATL's interest, as decided by the user department / Management on case-to-case basis.

In case of termination of a vendor due to any of the above reasons, the same cannot be on-boarded in ATL for undertaking any activity in future. Further, on an immediate basis, all existing activities provided by the vendor across ATL to be stopped. Alternative arrangements to be suggested as per the guidelines would be explored by the department in case discontinuation/termination is envisaged.

ATL reserves the right to declare a vendor ineligible, either indefinitely or for a stated period of time and/or reject a proposal for award, if at any time it arrives at the conclusion that the vendor has engaged in corrupt or fraudulent practices in competing for, or in executing the contract.

The termination procedure shall be initiated by Procurer team for their respective vendors as per the contract. The user departments shall ensure adequate documentation is made available pertaining to contract termination:

- Note detailing the reason for termination and approval of the departmental Head
- Performance assessment sent to the vendor seeking clarification
- Final termination letter sent to the vendor as per the draft approved by legal department

The respective Department may explore communicating the reason for termination to group with the reasons for termination, as required. Further, the records of such terminated vendors would be maintained, and contracts shall be closed in the system. Detailed procedure to be followed for the same is mentioned in the Annexure.

XII. Vendor Bill Processing

Vendors shall be responsible for submitting bills on time for payment processing. All bills pertaining to the procurement of non-IT for products / services should be submitted by Administration team / Procurer for bill verification. Similarly, bills related to procurement of IT products / services should be submitted by IT team for bill verification. If required, Administration team / Procurer & IT team can seek further clarification from concerned departments internally for bill verification. All bills received shall be verified within defined timeline by concerned teams (Administration team / Procurer / IT team).

All verified bills shall be forwarded to Finance & Accounts team for payment processing. F&A team shall complete the payment processing and release the payment to vendor within defined timeline.

XIII. Please note: In case the defined policy is not adhered the payment for all such procurements shall not be processed. For any exception, prior approval needs to be obtained from MD & CEO. **Vendor Risk Management Audit**

Regular audits by either the internal auditors or external auditors of the Company shall be done to assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the Company's compliance with its risk management framework. On an annual basis, review of the financial and operational condition of the service provider to access its ability to continue to meet its outsourcing obligations would be performed by the respective functional department.

Such due diligence/scorecard reviews, which can be based on all available information about the service provider shall highlight any deterioration or breach in performance standards confidentiality and security, and the business continuity preparedness.

Periodic review of vendors as further cyber, and information security (Includes data protection controls of data confidentiality) practices as laid down by ATL's Information Security management systems, frameworks, policies and technological system and controls to be equally followed by vendors to avoid leakage of customer's data.

Type of vendors	**Frequency of review**
Material /Critical Vendors	Half yearly
Non-material vendors	Annual

A robust system of internal audit of all outsourced activities shall be put in place and monitored by the Board of ATL.

ATL shall ensure to add clause of right to audit stating Regulator or any person so authorized by Regulator shall have right to conduct an inspection and audit by internal or external auditor so appointed by the Regulator or by ATL and examine the documents , records and transactions pertaining to ATL either stored or processed or within the custody of the Service Provider, the Service Provider shall, allow free access to the said Regulator or its authorised person either independently or along with the officials of the ATL to access the said records either in physical form at the place where it is stored or in any other form as it is stored or as it may be needed by the said Regulator or its authorised person.

XIV. Vendor Business Continuity Plan

ATL would ensure controls established for documenting, maintaining and testing business continuity and recovery procedures. The Business continuity framework developed by the vendor shall include:

- Requirement that vendor periodically tests the Business continuity and Recovery plan and may also consider occasional joint testing and recovery exercise with its service provider.
- Availability of alternate vendor or the possibility of bringing the outsourced activity back-in- house in an emergency and the cost, time and resources that would be involved.

- Availability of DR infrastructure to ensure continuity during any incident at primary data center, wherever dependency on vendor is for its applications

As per the ATL's BCM framework, all the critical activities require a robust business continuity plan to ensure recovery of critical activities within defined RTO and the vendor BCP is a subset of the ATL's overall BCP framework. The ATL's BCP plan will be evaluated to understand the dependency of vendors for the completion of ATL's critical activities. Vendors performing critical activities should establish a robust framework for documenting, maintaining and testing business continuity procedures and share their latest BCP/DR plan and Test report on an annual basis with the unit. It will be responsibility of the Business/Operations department to hold the test reports with them and submitted whenever sought by control functions. In order to reduce the inherent risk due to dependency on outsourced vendors, the relevant departments would evaluate alternative vendors for any critical outsourced activities or enhance the skills of their own staff to perform the critical activities during disruption or non-availability of vendor.

Identification of critical activities and thereof BCP for the Vendors performing these critical activities, will be jointly done by the department concerned and Business continuity team while conducting Business Impact Analysis as detailed in BCP policy of ATL. The team shall ensure that contingency plans, based on Business continuity requirements of ATL are documented and tested regularly.

XV. Vendor Client Interaction and Redressal of Grievances relating to Outsourced services

Irrespective of the outsourcing arrangement, the commitment, service delivery to the client is complete ownership of ATL. ATL will be responsible for the final delivery to the customer at all times. The said outsourcing agreement neither prevents nor impedes ATL from meeting its respective regulatory obligation, nor the regulator from exercising its regulatory powers.

The vendor should be made aware that interaction with ATL's customers can happen only with prior permission of the company. If allowed, the vendors will ensure that the interaction is conducted in a professional manner and internal information pertaining to ATL or any other client should be parted with at any point in time only on a need to know basis specific to the activity outsourced. The department of ATL, which has outsourced the activity, will be accountable at all times for regulatory compliance as well as customer complaints management and redressal. Customer complaints redressal would be continued as per the various customer grievance redressal channels in ATL and all complaints would be redressed immediately and within an outer timeline of 10 days from the date of receipt of the complaint.

Vendors handling sensitive information: Confidentiality and security

Comprehensive data loss/leakage prevention strategy to be adhered by outsourcing vendors as per the Company's requirements:

 Controls to ensure preservation and protection of the security and confidentiality of customer information in the custody or possession of vendor.

 Access to customer information by staff of the vendor would be on 'need to know' basis i.e. limited to those areas where the information is required in order to perform the outsourced function.

 Controls implemented to isolate and clearly identify Company's customer information, documents, records, and assets to protect the confidentiality of the information. Further, the vendor would have strong safeguards so that there is no co-mingling of information/ documents, records and assets with other PSOs.

 Outsourcing arrangements will not affect the rights of the customer against the Company, including the ability of the customer to obtain redress as applicable under relevant laws. In cases where the customers are required to deal with the vendor in the process of dealing with ATL, the respective department shall incorporate a clause in the relative product literature/ brochure, etc., stating that they may use the services of agents in sales/ marketing etc. of the products. The role of agents may be indicated in broad terms.

XVI. Sub-Contracting

Sub-Contracting refers to an arrangement whereby the Vendor engaged by ATL further outsources a part of its activity to another vendor ("Sub Contractor"). Also, if a Vendor subcontracts its activities, responsibilities and obligations to another party, it remains accountable thereon in addition to being accountable for the risks posed by the actions / omissions of the other party to whom it has subcontracted. Vendor would seek prior approval of ATL (relevant department, outsourcing the activity) for use of sub-contractors for all or any part of the outsourced activity. Business unit to ensure due diligence of the sub-contractor as would be done for the vendor. Review of Sub-Contracted vendors to be part of the annual/half yearly exercise as per template.

XVII. Role of the Board/Risk Management Committee/Audit Committee of the Board

The Board of ATL or the Risk Management Committee of the Board would be responsible for:

- Approving a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the policies that apply to such agreements;
- Laying down appropriate approval authorities for outsourcing depending on risk and materiality;
- Setting up suitable administrative framework for senior management for the purpose of ensuring compliance with this Policy;

XVIII. Ultimate Responsibility & Accountability

The outsourcing of any activity by ATL does not diminish its obligations, and those of its Board/RMC and senior management, who have the ultimate responsibility for the outsourced activity.

Non-adherence of the policy and framework shall be reported to Ethics officer for suitable action as per the staff accountability framework.

Vendor Lifecycle Management Approval Process

Approval process includes multiple stages such as criticality assessment, Onboarding Approval, Periodic Review and termination. Outsourcing delegation shall be as per below depending on risks and criticality-

Type of activity as criticality	**Onboarding approval (including renewals)**	**Periodic Review**	**Termination**
Critical	MD&CEO	Department (Maker) – Any designation Checker-HOD	Department Head
Non-Critical	Department head (with half yearly review of vendor list by MD&CEO)	Maker- any designation Checker- SM and above	

XIX. Review and Exceptions

i. This Policy document will replace the existing Policy. Further, any exception to the Policy needs to be jointly approved by Risk, Compliance, Department head and CFO.
ii. The Policy will be reviewed and approved by the RMC and Board on an annual basis or as the need may arise. Any amendment to the Policy would be subject to review and approval by the Risk Management Committee (RMC) and Board of the Bank.
iii. In case of any amendments required either due to changes in RBI guidelines or any interim changes to be implemented immediately, the modifications can be approved by the ORMC. All the approved changes will be put up to the next RMC and Board for approval. Necessary amendments would be circulated to all the concerned departments.
iv. In addition, any changes to the annexures can be approved by the Compliance and Risk function.

****

ANNEXURE 1

1. Procedure for Product / Service Requisition & Vendor Identification

Activity	Description	Responsibility
Product/Service Requisition & Vendor Identification		
Product/Service Requirement Form	To raise a product or a service request to Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements	User Department
Seeking Complete Information	To check if the information is complete and optionally check if the product / service exist in the Product / Service Master list of CPT	Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements

Searching for vendors	• If the product / service does not exist in the current master list, to explore for new vendors and seek fresh quotations • If the product / service exists in the current master list, can check for the existing vendors along with their contracts or explore new vendors	Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements
Inviting quotations	To invite quotation from vendors To explore Reverse Auctioning seeking support from Bank Central Procurer wherever required	Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements
Cost benefit analysis	To prepare the note on cost benefit analysis based on quotations received from vendors. Minimum 3 quotations should be obtained from 3 different vendors for the required product / service, unless deviation from MD&CEO has been taken for the same. Exception: For Annual Maintenance Contract or IT commodity hardware, software, licenses, subscriptions; multiple quotations may not be required.	Procurer
Final Approval	The final shortlisted vendor to be placed before CFO and/or MD&CEO for final approval, in line with the delegation matrix. In case of auditor appointment, approval also to be sought from Compliance Head.	User Department

2. Procedure for Vendor Suspension / Termination

Vendor Suspension / Termination		
Performance evaluation	Vendor performance evaluation will be done at defined frequency depending on the criticality	Administration team / Procurer for non-IT related procurements & & IT team for all IT related procurements
Performance deviations	In case of deviation in performance in terms of quality, delivery, etc of product / service; feedback will be shared with vendor for seeking clarification and taking immediate corrective action	Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements
Repeated Performance deviations	In case of repeated performance deviations, legal team to be notified for taking adequate action in consultation with Senior Management	Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements
Termination / suspension of contract	Final termination letter/mail to be sent to the vendor	Legal team, Administration team / Procurer for non-IT related procurements & IT team for all IT related procurements

3. Required Forms & Formats

Below are the indicative forms and formats and can be modified as per business requirements from time to time.

Annexure 1

Vendor/Service Provider Application Form for Procurement and Outsourcing

(on the letter head of the entity)	
DETAILS OF THE SERVICE PROVIDER	
Name of the Service Provider	
Office Address	
Contact information Telephone No Email	
Name of the Contact Person	
Constitution	Sole Proprietorship/ Partnership/ Company/LLP
List of Mandatory Documents enclosed related to the constitution of the entity viz PAN, GST, Udyam, cancelled cheque, etc.	
Whether all the dues and compliances under statutory acts (GST, ISIS, Labour law, EPF, Bonus, Gratuity, etc. are done on time)	
B. OTHER DETAILS	
Prior / Existing relationship with A.TREDS Ltd, Axis Bank Ltd, and any other subsidiaries of Axis Bank Ltd.	
Existing/Potential Litigation against the concern	

Is the Proprietor/Partners/Directors owned or controlled by any director or officer/employee of A.TREDS Ltd., Axis Bank, Subsidiaries of Axis Bank or their relatives?	If yes, please specify details.
C. Activity Details	
Activity /(ies) to be handled:	
Business Continuity Plan of the Service Provider	
Does the activity to be handled is of critical nature?	
Do your processes, staff, systems providing services to A.TREDS reside out of India (if yes, pls provide details):	
Do you provide similar services to other TREDS entities, any entity engaged in Factoring business?	
D. Declaration	
I confirm that all the particulars given herein/above are true and correct.	
Name of the Service Provider:	
Name of the authorized signatory:	
Signature :	
Date:	

Annexure 2: Vendor/Service Provider Verification/Assessment Report

(To be filled in by the user department)

A.TREDS Ltd (ATL)	
Service Provider Verification Report	
Name of Proprietor/Partner/Director interviewed	
Interviewed on	
Interviewed by	
Service Provider Premises visited on	
Visited by	
	Comments of the visiting officer
Operating Office Address of the Service Provider which was visited	
Alternate Site Address of the Service Provider which was visited (As part of Business Continuity Preparedness) ATL staff to visit the operating office and the BCP location. (wherever applicable)	
Infrastructure Verification (To be specified if the Service Provider is using its own infrastructure to conduct the activity	
Check on IT systems being used	
Manpower check	
Check on Due Diligence Procedure adopted	
Check on Training Facilities	
Check on maintenance of Customer Data Confidentiality	
Check on facilities for storage of records	
Has there been an IS/IT Audit carried out by ATL/ External agency (Yes/ No) If Yes, Audit findings/Audit Report to be enclosed	
Name and Signature of the visiting Official	

Information Technology Checklist	
Name of the Service/activity to be Outsourced:	
Nature of service/activity outsourced:	

Name of the Service Provider/Vendor :	
Application Name:	
Application Functionality:	
Type of Vendor (Critical / Non-critical) and Reasoning	

Risk Management

Parameters	Remarks
1. Technical Risk and mitigation plans	
2. Network risk	
3. Any other risk envisaged	

Service Levels

Parameters	Remarks
1. Definition of the SLA of the product / service (TaT, Response, Resolve, etc.)	
2. Penalty in the case of breach	
3. Measurement period (Monthly / Quarterly / Yearly)	
4. Responsibility for measurement	
5. Reporting frequency and method	

Compliance to RBI Guidelines for material outsourcing

Parameters	Remarks
1. Adherence to ATL's security and Privacy Policy:	
2. Access control to ATL's systems, record and resources: ATL shall evaluate the adequacy of the internal controls environment offered by the service provider. Due consideration should be given to implementation by the service provider of various aspects like information system security policies and employee awareness of the same, logical access controls, physical and environmental security and controls, controls for handling data etc. (as applicable). ATL's need to take effective steps to ensure that risks with respect to confidentiality and security of data are adequately mitigated	
3. Independent audit and expert assessment : ATL should also periodically commission independent audit and expert assessments on the security and control environment of the service provider. If any exception is obtained (especially Critical vendors) then same should be documented.	
4. Business Continuity Plan: ATL should ensure that their business continuity preparedness is not compromised on account of outsourcing.	
5. Change Management and Monitoring controls: In the event of outsourcing of technology operations, the ATL should subject the same to enhanced and rigorous change management and monitoring controls since ultimate responsibility and accountability rests with the ATL.	
6. Contingency Plan: ATL, while framing the viable contingency plan, need to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in-house in an emergency and the costs, time and resources that would be involved and be prepared to take quick action, if warranted.	

7. Right to audit: ATL should ensure to add clause of right to audit stating Regulator or any person so authorised by Regulator shall have right to conduct an inspection and audit by internal or external auditor so appointed by the Regulator or by ATL and examine the documents , records and transactions pertaining to ATL either stored or processed or within the custody of the Service Provider, the Service Provider shall, within 24 hours from the said intimation and without demur, allow free access to the said Regulator or its authorised person either independently or along with the officials of the ATL to access the said records either in physical form at the place where it is stored or in any other form as it is stored or as it may be needed by the said Regulator or its authorised person.	

Name & signature of Head of User Department

Annexure 3 : Template for Review of Service Provider/vendor

(To be filled in by the user department)

General Information	Description
Date	
Department	
Name of the Service Provider/vendor	
Activity handled	
Location Serviced	
Review Period	

Performance Review		Response from user Department
Performance against agreed objectives	Good Satisfactory Poor	
Number and details of complaints received for products / services provided, against the service provider by the customer and resolution status	Nil	
Frauds Committed	Yes No If yes, specify details	
Compliance Breaches observed/ Breach of SLA	Yes No If yes, specify details	
Any customer data / financial / external losses or breaches suffered by ATL due to malpractice at the service provider end	No Yes If yes, please provide the following details and current status 1. Date of incidence 2. Nature of incidence 3. Breaches observed	

Performance Review		Response from user Department
	4. Amount of financial loss suffered by ATL 5. Amount Recovered 6. Amount pending for Recovery 7. Time required to recover the balance amount 8. Impact of ATL's reputation and brand value 9. Action taken by the department 10. Any other remarks	
Any adverse finding during the audit/review of the service provider	No Yes If, yes, Action taken by the department to correct the critical audit findings.	

FINANCIAL SOUNDNESS		Response from user Department
Any adverse findings on the financial condition of the Service Provider from Market sources (to be done annually for Critical vendors)	Yes No	
Is the Service Provider stable to continue its operation for ATL (to be done annually for Critical vendors)	Yes No	

BUSINESS CONTINUITY PREPAREDNESS		Response from user Department
Any partial/full disruption of the activity observed during the review period	Yes No	
Any alternate Service Provider available at the same location who can take up the activity in case of the present Service Provider being non-functional	Yes No	
Any occurrences of data loss/system failure at the Service provider end during the review period	Yes No	
Any material gaps identified in the Process/Policy/SLA:		

Performance Review	Response from user Department
Report on Annual Stress testing performed at the Service Provider end to test the Business Continuity Preparedness: Critical services & System identified for BCP/ DR :	
Recommendation by the Proposer	Review and Continue
Conditions in case of Conditional Continuance and rationale for the same	
Name of the user department official with designation	
Signature of the user department official and date	
Name of the user department head with designation	
Signature of the user department head and date	