



Utkarsh Small Finance Bank

POLICY FOR OUTSOURCING OF FINANCIAL AND IT SERVICES

Version 8.0 (September 23, 2023)

Contents

1. BACKGROUND	4
2. APPLICABILITY	4
3. DEFINITION	4
3. ACTIVITIES THAT CANNOT BE OUTSOURCED	5
4. COMMON AREAS OF OUTSOURCING	5
a) Banking Operations (Financial Outsourcing)	5
b) IT Operations	6
Services / Activities not considered under Outsourcing of IT Services	6
5. FRAMEWORK FOR APPROVAL	6
6. ROLE AND RESPONSIBILITY OF OUTSOURCING COMMITTEE	8
6.1 Regulatory and Supervisory requirements	8
6.2 Due diligence on service providers	9
6.3 Aspects to be considered in Due diligence.....	9
7. ROLE OF IT FUNCTION.....	10
8. OUTSOURCING AGREEMENT	10
8.1 Aspects to be considered in agreement	10
8.2 Termination clause.....	12
8.3. Sub-Contracting.....	12
8.4. Dispute resolution	13
8.5. Applicable laws.....	13
9. OUTSOURCING WITHIN A GROUP AND OFF-SHORE	13
9.1 Outsourcing within a group/ Conglomerate	13
9.2 Off-shore outsourcing of financial and IT services (Outsourcing to Foreign Service providers).....	13
9.3 The outsourcing related to overseas operations of Bank	14
10. CONTROL ENVIRONMENTS OFFERED BY THE SERVICE PROVIDER	14
10.1 Confidentiality and security.....	15
10.2 Responsibilities of DSA/ DMA/ recovery agents	15
11. MONITORING AND CONTROL OF OUTSOURCED ACTIVITIES	15
11.1 Structure for management and control of Outsourcing	15
11.2 Service level agreements and performance metrics	16
11.3 Measuring by key performance indicators (KPIs).....	16
12. BUSINESS CONTINUITY AND MANAGEMENT OF DISASTER RECOVERY PLAN	17

13. GRIEVANCES RELATING TO OUTSOURCED SERVICES	18
14. RISK EVALUATION AND MEASUREMENT	18
14.1 Framework for risk evaluation	18
14.2 Area of risk evaluation.....	19
15. PERIODIC RISK ASSESSMENT, AUDIT AND REVIEWS	20
15.1 Review of outsourcing arrangements.....	20
16. OTHER MANDATORY REGULATORY REQUIREMENTS.....	21
17. REPORTING TO INDIAN BANKS ASSOCIATION	21

1. BACKGROUND

Utkarsh Small Finance Bank Limited is a subsidiary promoted by Utkarsh Core Invest Limited formerly known as Utkarsh Micro Finance Limited. It aims to provide affordable & accessible banking services which are process centric, technology enabled, and people oriented resulting in reliable, scalable, and sustainable institution facilitating socio-economic changes. The purpose is to provide Banking products to the unserved and underserved sections of the country, which includes small and marginal farmers, micro and small industries, and other organized sector entities, at an affordable cost. The Bank's vision is "To be the most trusted, digitized bank that is financially and socially inclusive, and creates value across social strata through insightful and viable solutions".

Bank engages service provider to manage certain activities, on behalf of/ for the Bank, on a continual basis that includes activities like data processing, business correspondents, DSA, etc., these are governed by below mentioned guidelines:

RBI guidelines viz. DBOD.NO.BP.40/21.04.158/2006-07 dated November 3, 2006 and DBR.No.BP.BC.76/21.04.158/2014-15 dated March 11, 2015 on "Guidelines on Managing Risk and Code of Conduct in Outsourcing of Financial Services by Bank" and DoS.CO. CSITEG/SEC.1/31.01.015/2023-24 dated April 10, 2023 on "Master Direction on Outsourcing of Information Technology Services".

2. APPLICABILITY

This policy is governed by guidelines mentioned above and follows the broad principles and processes adopted for appointment of service provider for outsourcing of financial activities and IT operations in the Bank.

This Policy is not applicable for activities which are not related to banking services like usage of courier, catering of staff, housekeeping and janitorial services, security of the premises etc.

In cases of any conflict between this policy and Regulatory guidelines issued within India, the more stringent of the two would prevail.

3. DEFINITION

- a) **Outsourcing** - It can be defined as Bank's 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 continuous basis that would normally be undertaken by the Bank itself, now or in the future.
- b) **Material Outsourcing of IT Services** are those which:
 - i) if disrupted or compromised will have the potential to significantly impact the Bank's business operations; or
 - ii) may have material impact on the Bank's customers in the event of any unauthorised access, loss or theft of customer information.
- c) **Outsourcing of IT Services** - Outsourcing of IT Services shall include outsourcing of the activities like
 - (i) IT infrastructure management, maintenance and support (hardware, software or firmware); (ii) Network and security solutions, maintenance (hardware, software or firmware); (iii) Application Development, Maintenance and Testing, Application Service Provider(ASPs) including ATM Switch ASPs; (iv) Services and operations related to Data Centers; (v) Cloud Computing Services (vi)

Managed Security Services and (vii) Management of IT infrastructure and technology services associated with payment system ecosystem.

- d) **Service Provider** - It means the provider of IT or IT enabled services including entities related to the Bank or those which belong to the same group or conglomerate to which the Bank belongs. Appendix III provides an indicative (but not exhaustive) list of:
- i) Services/ Activities not considered under "Outsourcing of IT Services" for the purpose of IT Outsourcing – Refer Appendix III
 - ii) Vendors / entities who are not considered as Third Party Service Provider (TPSP) for the purpose of IT Outsourcing – Refer Appendix III
- e) **Financial Outsourcing** – Typically outsourced financial services include applications processing (loan origination, credit card) document processing, marketing and research, supervision of loans, data processing and back office related activities, etc.
- f) **Sub-Contracting** - Subcontracting refers to an arrangement whereby the outsourced agency engaged by the Bank further outsources a part of its activity to another service provider (Sub contractor).

3. ACTIVITIES THAT CANNOT BE OUTSOURCED

Bank will not outsource any activities which are prohibited under applicable legal, regulatory or statutory requirements. The Bank, through the Operational Risk team will ensure that activities like, Core management functions viz., Internal audit and the Compliance function, execution of orders and monitoring of trading activities of clients, decision - making functions like determination of compliance with KYC norms for opening deposit accounts, according sanction for loans (including retail loans) and management of investment portfolios are not outsourced.

For the purpose of Core Business Functions, these are those functions which are vital for the Bank without which it cannot survive and/ or effectively achieve its objectives. These functions are specific to the Bank and helps differentiate the Bank from competition and involve decision making at the highest levels. These functions may include functions like Business Strategy, Pricing -Client services, Client Relationship Management, Product Design and Management, Management of Intellectual Property. The Board of the Bank may approve outsourcing of core business activities or functions on the basis the business benefits after Risk Management committee has evaluated associated risks and other factors as laid down in the policy.

4. COMMON AREAS OF OUTSOURCING

Financial and IT Outsourcing - All financial and IT Services outsourcing would be under the purview of the policy irrespective of its material impact. Typical activities under financial outsourcing and IT operations includes:

a) Banking Operations (Financial Outsourcing)

- i) Leads generation for sourcing of business.
- ii) Application processing (Loan Origination, Credit Card).
- iii) Supervision of loans.
- iv) Cash management and Collections.
- v) Customer service helpdesk/ call center services.
- vi) Document/ Data/ Transaction Processing including payments, loans, deposits.

- vii) Activities such as Debit card printing and dispatch, verifications.
- viii) Back office related activities etc.
- ix) Marketing and research.
- x) Fiduciary and trading activities.
- xi) Partnership based Fintech firms such as those providing co-branded applications, service, products.
- xii) Reconciliation of transactions between the Bank and service provider

b) IT Operations

- i) Technology infrastructure management, maintenance and support.
- ii) Application development, maintenance and testing.
- iii) Cloud Computing Services

Services / Activities not considered under Outsourcing of IT Services

- i) Corporate Internet Banking services obtained by bank as corporate customers/ sub members of another Bank.
- ii) External audit such as Vulnerability Assessment/ Penetration Testing (VA/PT), Information Systems Audit, security review.
- iii) SMS gateways (Bulk SMS service providers).
- iv) Procurement of IT hardware/ appliances.
- v) Acquisition of IT software/ product/ application (like CBS, database, security solutions, etc.,) on a license or subscription basis and any enhancements made to such licensed third-party application by its vendor (as upgrades) or on specific change request made by the Bank.
- vi) Any maintenance service (including security patches, bug fixes) for IT Infra or licensed products, provided by the Original Equipment Manufacturer (OEM) themselves, in order to ensure continued usage of the same by the Bank.
- vii) Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.
- viii) Platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.
- ix) Any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the Bank wherein only a license is procured with no / minimal customization.
- x) Services obtained by a bank as a sub-member of a Centralized Payment Systems (CPS) from another Bank.
- xi) Business Correspondent (BC) services, payroll processing, statement printing.
- xii) This is an indicative but not exhaustive list.

5. FRAMEWORK FOR APPROVAL

Proposals for review of the outsourced activities to the service provider must be carried out annually by the Committee set up for this purpose.

Before on-boarding, vendor shall provide Risk Assessment Template in Annexure 1 format. The Annexure 1 filled by vendor for onboarding shall be submitted to Operational Risk (OR) team prior to placing the Vendor application to the Outsourcing Committee. On the basis of information/data provided by vendor in Risk Assessment Format (Annexure 1) Operational Risk team will provide Risk Scoring for the Vendor.

The ORMC of the Bank would assess, quantify, and review the risk mitigations measures being put in place for outsourced financial and technology services irrespective of the materiality. The Bank through

its respective outsourcing department, will have the ultimate responsibility for the outsourced activity. The outsourcing of any activity would not diminish the obligation of the Bank in respect of that activity. The roles and responsibilities and the composition of the Committee are described below:

The Executive Committee (EC) will be empowered to effect any changes in the composition of the 'Outsourcing Committee' of the Bank in adherence with applicable regulatory guidelines.

Members: Roles and Responsibilities

Members	Roles and Responsibilities
Head –Operations (Chairperson)	To examine the aspects relating to operations. The Chairperson to ensure that the Outsourcing Committee functions properly, that all relevant matters are discussed and that effective decisions are made and carried out. He also coordinates with the committee to ensure that appropriate policies and procedures are in place for effective management of the organisation.
Head – Branch & Assets Operations (Convener)	To coordinate for convening the meeting and maintaining records and documentation related to on boarding and reviews outsourced vendor partners.
Chief Financial Officer (CFO)	Evaluation of financial soundness of the outsourced agency.
Chief Information Officer (CIO) / Suitable nomination from IT	Examine the aspects relating to information technology services and operations.
Chief Compliance Officer (CCO)	Examine the regulatory impact including statutory compliance and convey the regulations to be complied with. Provide appropriate clauses in the service level agreement to cover all the necessary regulatory and risk mitigation measures in line with Bank's Outsourcing Policy.
Chief Human Resource Officer (CHRO)	To examine the human aspects relating to Onboarding outsource vendor partners.
Chief Information Security Officer (CISO)	Examine the aspects relating to Information Security services and operations.
Chief Risk Officer (CRO)	To evaluate proposals from a Risk perspective and furnish his inputs wherever the Bank is outsourcing any of its activities
HODs having Outsourced activities (To participate as presenter)	Arrange for Onboarding and managing the service providers including review of outsourcing contracts Annually and submission to Outsourcing committee.

6. ROLE AND RESPONSIBILITY OF OUTSOURCING COMMITTEE

6.1 Regulatory and Supervisory requirements

- i) Outsourcing of any activity will not diminish the Bank's or Board's or Senior Management's responsibility for the outsourced activities. The Bank will take steps to ensure that the service provider employs the same high standard of care in performing the services as would have been employed by the Bank, if the same activity was not outsourced. Bank will not engage an IT service provider that would result in reputation of the Bank being compromised or weakened. All outsourcing arrangements would adhere to the following broad guidelines that should be monitored by the Outsourcing committee during reviews.
- ii) Notwithstanding whether the service provider is located in India or abroad, the Bank will ensure that the outsourcing is neither impeded nor interfered with the ability of the Bank to effectively oversee and manage its activities. Further, the Bank will ensure that the outsourcing not impede the RBI in carrying out its supervisory functions and objectives.
- iii) The Bank will ensure that the service provider, if not a group company, will not be owned or controlled by any director, or key managerial personnel, or approver of the outsourcing arrangement of the Bank, or their relatives. The terms 'control', 'director', 'key managerial personnel', and 'relative' has the same meaning as assigned under the Companies Act, 2013 and the Rules framed thereunder from time to time. Any exception to this requirement will be made with the approval of Board/ Board level Committee and with appropriate disclosure, oversight and monitoring of such arrangements. The Board will inter-alia ensure that there is no conflict of interest arising out of third-party engagements.
- iv) Additional requirements pertaining to usage of cloud computing services and outsourcing of Security Operations Center (SOC) services are outlined in Appendix I and Appendix II, respectively.
- v) Compliance to all relevant laws, regulations, guidelines, and conditions of approval, licensing, or registration etc., will be fulfilled. f) The grievance redressal mechanism needs to be robust in the Bank and will not compromise on account of outsourcing i.e. responsibility for redressal of customer's grievances related to outsourced services will be with the Bank. Outsourcing arrangements shall not affect the rights of a customer against the Bank, including the ability of the customer to obtain redressal as applicable under relevant laws.
- vi) Bank would evaluate the need for Outsourcing of IT Services based on comprehensive assessment of attendant benefits, risks and availability of commensurate processes to manage those risks. Bank would inter-alia consider the need for outsourcing based on criticality of activities to be outsourced, determining expectations and outcome from outsourcing, determining success factors and cost-benefit analysis and deciding the model for outsourcing.
- vii) Outsourcing of services relating to credit cards would be as per the detailed instructions contained in RBI Circular (RBI/2022-23/92DoR.AUT.REC.No.27/24.01.041/2022-23 dated April 21, 2022) and RBI guidelines on Recovery Agents engaged by Banks conveyed vide RBI/2007-2008/296 DBOD.No.Leg.BC.75 /09.07.005/2007-08 dated April 24, 2008. The code of conduct for Direct Sales Agents (DSAs) will be as per "Model code of conduct for DSAs circulated by IBA.
- viii) The respective vertical of the Bank who proposed for on-boarding the outsourcing agency, would create an inventory of services provided by the service providers (including key entities involved in their supply chains). Further, Bank would map their dependency on third parties and

periodically evaluate the information received from the service providers and present for further review by the Outsourcing Committee.

6.2 Due diligence on service providers

Comprehensive due diligence on the nature, scope and complexity of the outsourcing should be performed. Identify the key risk and risk mitigation strategies. e.g. in case of technology outsourcing, the state of security practices and controls environment offered by the service provider is a key factor.

Outsourcing agreement should include, oversight and management of third-party vendor's/ service providers & partners. While conducting the due diligence on service providers, consideration should be given to the below mentioned points:

- i) In considering or renewing an Outsourcing of IT Services arrangement, appropriate due diligence will be performed to assess the capability of the service provider to comply with obligations in the outsourcing agreement on an ongoing basis.
- ii) A risk-based approach will be adopted in conducting such due diligence activities.
- iii) Due diligence will take into consideration qualitative, quantitative, financial, operational, legal and reputational factors. The Bank will obtain independent reviews and market feedback on the service provider to supplement its own assessment as per business requirements.
- iv) The Bank will also consider, while evaluating the capability of the service provider, risks arising from concentration of outsourcing arrangements with a single or a few service provider/s.

6.3 Aspects to be considered in Due diligence

Due diligence will involve evaluation of all available information, as applicable, about the service provider, which includes:

- i) Past experience and competence to implement and support proposed activities over the contractual period.
- ii) Financial soundness and ability to service commitments even under adverse conditions.
- iii) Business reputation and culture, compliance, complaints and outstanding or potential litigations.
- iv) Conflict of interest, if any.
- v) Security and internal control and monitoring environment, business continuity management
- vi) External factors like political, economic, social, and legal environment of jurisdiction in which the service provider operates and other events that may impact service Performance.
- vii) Details of technology, infrastructure stability, security and internal control, audit coverage, reporting and monitoring procedures, data backup arrangements, business continuity management and disaster recovery plan.
- viii) Capability to identify and segregate Bank's data.
- ix) Due diligence for sub-service providers.
- x) Risk management, framework, alignment to applicable international standards on quality/ security/ environment etc., may be considered.
- xi) Capability to comply with regulatory and legal requirements of the outsourcing of IT Services arrangement.
- xii) Information/ cyber security risk assessment.

- xiii) To ensure appropriate controls, assurance requirements and possible contractual arrangements are in place to ensure data protection and the Bank's access to the data which is processed, managed or stored by the service provider.
- xiv) Secure infrastructure facilities.
- xv) Employees training and knowledge transfer.
- xvi) Ability to effectively service all the customers while maintaining confidentiality, especially where a service provider has exposure to multiple entities. quality of due diligence exercised by the service provider with respect to its employees and sub-contractors.
- xvii) The nature of the legal relationship between the parties will be considered i.e. Whether agent, principal or otherwise. The contract should clearly define what activities are going to be outsourced including appropriate service and performance standards.
- xviii) The outsourcing agreement should provide provision for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard.

Extent of due diligence reviews may vary based on risk inherent in the outsourcing arrangements. Due diligence undertaken during the selection process, by various verticals of the Bank, should be documented and re-performed periodically as part of the monitoring and control processes of outsourcing through the Outsourcing Committee meeting. Outsourcing and Vendor risk management team should ensure to obtain independent reviews and market feedback to supplement internal findings. Outsourcing and Vendor risk management team should ensure that information used for due diligence is current and not more than 12 months old.

7. ROLE OF IT FUNCTION

Role of IT Function has been covered under this IT Policy and IT Department shall ensure, inter alia, (a) assisting the Senior Management in identifying, measuring, monitoring, mitigating and managing the level of IT outsourcing risk in the organisation; (b) ensuring that a central database of all IT outsourcing arrangements is maintained and is accessible for review by Board, Senior Management, Auditors and Supervisors; (c) effectively monitor and supervise the outsourced activity to ensure that the Service Providers meet the laid down performance standards and provide uninterrupted services, report to the Senior Management; co-ordinate periodic due diligence and highlight concerns, if any; and (d) putting in place necessary documentation required for contractual agreements including service level management, monitoring of vendor operations, key risk indicators and classifying the vendors as per the determined risk.

8. OUTSOURCING AGREEMENT

The Outsourcing can be done only after execution of the legally binding written agreement between the Bank and vendor duly vetted by the Bank's legal department on their legal effect and enforceability. Agreement with the service provider would be executed as per standard format and any deviation should require specific approval by the Outsourcing Committee. Amendments to the agreement should be carried out as a supplementary to the agreement.

8.1 Aspects to be considered in agreement

- i) The contract should detail the activity being outsourced, including appropriate service and performance standards, and penalties, including those for the sub-contracts, if any.
- ii) The contract should mention the deliverables in the Service Level Agreement (SLA) to measure the quality and quantity of the services.

- iii) The contract should mention that the data storage is to be done only in India as per extant regulatory requirements though a notification from RBI RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018 dated April 06, 2018.
- iv) The Legal and the IT department of the Bank should ensure that the contract brings out nature of legal and regulatory relationship between the parties (agent, principal or otherwise), and addresses risks and mitigation strategies identified at the risk evaluation and due diligence stages. Contracts should clearly define the roles and responsibilities of the parties to the contract and include suitable indemnification clauses. Any 'limitation of liability' consideration incorporated by the service provider should be assessed in consultation with the legal department.
- v) The type of material adverse events (e.g., data breaches, denial of service, service unavailability, etc.) and the incidents required to be reported to Bank to enable the Bank to take prompt risk mitigation measures and ensure compliance with statutory and regulatory guidelines.
- vi) Controls for maintaining confidentiality of data of the Bank and its customers' and incorporating service provider's liability to the Bank in the event of security breach and leakage of such information.
- vii) Contracts should provide for periodic renewal and re-negotiation to enable the Bank to retain an appropriate level of control over the outsourcing and should include the right to intervene with appropriate measure to meet the Banks' legal and regulatory obligations.
- viii) Types of data/ information that the service provider (vendor) is permitted to share with the Bank's customer and / or any other party.
- ix) The contract must specify the resolution process, events of default, indemnities, remedies, and recourse available to the respective parties, contingency plan(s) to ensure business continuity and testing requirements.
- x) The contract must enable the Bank with the ability to access all books, records and information relevant to the outsourced activity available with the service provider.
- xi) The contract should mention compliance with the provisions of the Information Technology Act, 2000, other legal requirements and standards to protect the customer data.
- xii) Clauses requiring the service provider to provide details of data (related to the Bank and its customers) captured, processed and stored.
- xiii) The contract should provide the Bank with the right to conduct audits on the service provider whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the Bank.
- xiv) Right to seek information from the service provider about the third parties (in the supply chain) engaged by the former.
- xv) Recognizing the authority of regulators to perform inspection of the service provider and any of its sub-contractors. Adding clauses to allow RBI or person(s) authorized by it to access the Bank's IT infrastructure, applications, data, documents, and other necessary information given to, stored or processed by the service provider and/ or its sub-contractors in relation and as applicable to the scope of the outsourcing arrangement.
- xvi) Including clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractors.
- xvii) Obligation of the service provider to comply with directions issued by the RBI in relation to the activities outsourced to the service provider, through specific contractual terms and conditions specified by the Bank.
- xviii) Clauses requiring prior approval/ consent of the Bank for use of sub-contractors by the service provider for all or part of an outsourced activity
- xix) Termination rights of the Bank, including the ability to orderly transfer the proposed IT-outsourcing arrangement to another service provider, if necessary or desirable;
- xx) The contract should include a clause requiring non-disclosure agreement with respect to information retained by the service provider.

- xxi) Regular monitoring and assessment of the service provider by the Bank for continuous management of the risks holistically, so that any necessary corrective measure can be taken.
- xxii) Provision to consider skilled resources of service provider who provide core services as “essential personnel” so that a limited number of staff with back-up arrangements necessary to operate critical functions can work on-site during exigencies (including pandemic situations);
- xxiii) Clause requiring suitable back-to-back arrangements between service providers and the OEMs
- xxiv) Obligation of the service provider to comply with the directions issued by Reserve Bank of India (RBI) in relation to the activities outsourced by the Bank.

8.2 Termination clause

- i) Contracts should include a termination clause and minimum periods to execute a termination provision, as deemed necessary, while maintaining the business continuity during and after termination, provided the outsourced activity is to be continued. Contract should provide for maintaining confidentiality of customer's information even after the contract expires or is terminated by either party. Further, the agreement shall have necessary clauses on data privacy, data protection, safe removal/ destruction of data, hardware and all records (digital and physical), as applicable. However, service provider shall be legally obliged to cooperate fully with both the Bank and new service provider(s) to ensure there is a smooth transition. Further, agreement shall ensure that the service provider is prohibited from erasing, purging, revoking, altering or changing any data during the transition period, unless specifically advised, in writing, by the regulator or the Bank.
- ii) Contract should include conditions for default termination/ early exit option for contracts. This may include circumstances when the service provider undergoes a change in ownership becomes insolvent or goes under liquidation, received judicial indictment (whether within India or any other location) or when there has been a breach of confidentiality, security, or demonstrable deterioration in quality of services rendered.
- iii) In all cases of termination (early or otherwise) an appropriate handover process for data and process needs to be agreed with the service provider.
- iv) In the event of termination of outsourcing agreement, in any case where the service provider deals with the customers of the Bank, the same shall be given due publicity by the Bank so as to ensure that the customers stop dealing with that concerned service provider. List of terminated cases and IBA caution list would be uploaded on the Bank's website and intranet. Business Heads should ensure that service of outsourced agencies which are included in 'Caution List' of Indian Banks Association should not be availed
- v) In case of cloud computing services, exit / termination plans should ensure how the cloud hosted service(s) and data will be moved out from the cloud with minimal impact on continuity of the bank's business, while maintaining integrity and security.

8.3. Sub-Contracting

Agreements may include covenants limiting further sub-contracting. Agreements should provide for due prior approval/ consent by the bank of the use of subcontractors by the service provider for all or part of an outsourced activity. The Bank should retain the ability of similar control and oversight over the sub service provider as the service provider.

Provided that such contract should provide for the prior approval/consent by the Bank of the use of subcontractors by the service provider for all or part of an outsourced activity. Bank to conduct audit of the service provider including its sub-contractors) whether by its internal or external auditors, or by agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made about the service provider in conjunction with the services performed.

8.4. Dispute resolution

Agreements should specify the resolution process, the event of default, indemnities involved and the remedies and recourse of the respective parties to the agreement.

8.5. Applicable laws

Agreements should be based on the regulations applicable to the Bank. An agreement should be tailored to provide for specific risks relating to cross border businesses and operations, data privacy and ownership aspects among others.

9. OUTSOURCING WITHIN A GROUP AND OFF-SHORE

9.1 Outsourcing within a group/ Conglomerate

These guidelines are generally applicable to outsourcing within a group/ conglomerate, including Head Office, Zonal Office/ Regional office, administrative offices or Branch office of the company whether located within or outside India and such an arrangement shall be backed by this Policy and appropriate service level arrangements with its group entities. These requirements may be addressed as part of group wide risk assessment and management procedures.

The selection of a group entity shall be based on objective reasons that are similar to the selection of a third-party, and any conflict of interest that such an outsourcing arrangement may entail shall be appropriately dealt with.

The Bank at all times, shall maintain an arm's length relationship in dealings with their group entities. Risk management practices being adopted by the Bank while outsourcing to a group entity shall be identical to those specified for a non-related party.

Due diligence in an intra-group service provider may take the form of evaluating qualitative aspects of the ability of the service provider to address risks specific to the Bank.

9.2 Off-shore outsourcing of financial and IT services (Outsourcing to Foreign Service providers)

The Bank shall closely monitor government policies of the jurisdiction in which the service provider is based and the political, social, economic and legal conditions on a continuous basis, as well as establish sound procedures for mitigating the country risk. This includes, *inter alia*, having appropriate contingency and exit strategies. Further, it would be ensured that the availability of records to the Bank and the RBI will not be affected even in case of liquidation of the service provider. Further, the governing Law of the arrangement shall also be clearly specified. In principle, arrangements will only be entered into with parties operating in jurisdictions upholding confidentiality clauses and agreements.

Further, the Bank and the RBI possess the right to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction and the arrangement shall comply with all statutory requirements as well as regulations issued by the RBI from time to time.

Also, the activities outsourced outside India should be conducted in a manner so as not to hinder efforts to supervise or reconstruct the Indian activities of the Bank in a timely manner.

To manage the country risk involved in such outsourcing activities, Outsourcing and Vendor risk management team should take into account and closely monitor government policies and political, social, economic and legal conditions in countries where the service provider is based, during the risk assessment process and on a continuous basis and establish sound procedures for dealing with country risk problems.

Legal department shall ensure the following clauses are present in the Agreement:

- i) Bank should principally enter arrangements with parties operating in jurisdictions that generally uphold confidentiality clauses and agreements. The governing law of the arrangement should also be clearly specified.
- ii) Bank should not outsource within jurisdictions where access to books, records and any other information required for audit and review purposes may be impeded due to regulatory or administrative constraints.
- iii) The right of the Bank and the RBI to direct and conduct audit or inspection of the service provider based in a foreign jurisdiction.
- iv) Emerging technologies such as data center hosting, applications as a service, cloud computing have given rise to unique legal jurisdictions for data and cross border regulations. Banks should clarify the jurisdiction for their data and applicable regulations at the outset of an outsourcing arrangement. This information should be reviewed periodically and in case of any significant changes performed by the service provider.

9.3 The outsourcing related to overseas operations of Bank

The outsourcing related to overseas operations of bank would be governed by both these guidelines and the host country guidelines. Where there are differences, the more stringent of the two would prevail. However, where there is any conflict, the host country guidelines would prevail.

10. CONTROL ENVIRONMENTS OFFERED BY THE SERVICE PROVIDER

Outsourcing and Vendor risk management team should ensure to evaluate the adequacy of internal controls environment offered by the service provider. Due consideration should be given to the implementation of following by the service provider:

- i) Information security policies and employee awareness of the same.
- ii) Controls implemented for logical access to customer information by service provider staff, so that information may be accessed on a need-to-know basis only.
- iii) Physical and environmental security and controls.
- iv) Network security and controls.
- v) Formal process for tracking and monitoring program changes and projects.
- vi) Process for incident reporting and problem management.
- vii) Special control considerations for service providers using cloud computing as part of service.

- viii) Control considerations for handling of customer information and personally identifiable Information.
- ix) Data classification and controls for handling data
- x) Assurance mechanisms by service provider (e.g., relevant ISO certifications, ISAE SOC 1 and 2 attestations, periodic security testing and audits conducted by CERT-In empaneled vendors, etc.).

10.1 Confidentiality and security

- i) Outsourcing agreement should mandate controls to ensure customer data confidentiality and service provider's liability in case of breach of security and leakage of confidential customer related information. e.g., use of transaction-enabled mobile banking channels necessitates encryption controls to ensure security of data in transmission.
- ii) Outsourcing agreement should mandate controls to provide for the preservation of documents and data by the service provider in accordance with the legal/regulatory obligation of the bank in this regard.

10.2 Responsibilities of DSA/ DMA/ recovery agents

Relevant department hiring DSA/ DMA/ Recovery agents would ensure the following:

- i) Direct Sales Agents (DSA)/ Direct Marketing Agents (DMA)/ Recovery Agents are trained to handle customers with care and sensitivity, particularly while soliciting customers by adhering to hours of calling, maintain privacy of customer information and convey the terms and conditions of the products.
- ii) Recovery Agents adheres to instructions on Fair Practices Code for lending (Circular DBOD. Leg. No.BC. 104 /09.07.007/2002-03 dated May 05, 2003) as also their own code for collection of dues.
- iii) Recovery agents should refrain from action that could damage the integrity and reputation of the Bank and would observe strict customer confidentiality.
- iv) Recovery Agents do not resort to intimidation or harassment of any kind, either verbal or physical against any person in their debt collection efforts.
- v) Department outsourcing the activity, should ensure that any deviations from the above-mentioned terms are updated to Outsourcing Committee within 7 days along with the details of the incident and action taken against the service providers.

11. MONITORING AND CONTROL OF OUTSOURCED ACTIVITIES

11.1 Structure for management and control of Outsourcing

The Operational Risk team should ensure to establish a structure for management and control of outsourcing, based on the nature, scope, complexity and inherent risk of the outsourced activity. A structure for monitoring and control of outsourced activities should comprise of the following:

- i) A centralized record of all material outsourcing, including technology outsourcing and sub service provider relationships, that is readily accessible for review by the Board and Senior Management of the Bank will be maintained. The Bank will conduct regular audits of service providers with regard to the service outsourced by it and such audit may be conducted either by the internal auditor of the Bank or external auditors appointed to act on Bank's behalf and such audit may be in the form of shared audit if the same service provider is providing services to more than one Bank. Further, the records should be updated promptly, and half yearly review should be placed before the Board.

- ii) During the audit, the Bank shall assess the performance of the service provider, adequacy of the risk management practices adopted by the service provider, compliance with laws and regulations, etc. with support from the Legal department, as and when required.
- iii) Information Security team should review and monitor the security practices and control processes of the service provider on a regular basis and require the service provider to disclose security breaches. Also, the report on monitoring and control activities shall be reviewed periodically by the Outsourcing Committee and in case of any adverse development or non-compliance with legal and regulatory requirements in an outsourcing arrangement, the same shall be intimated to the Board through RMCB and RBI for information.
- iv) The Bank shall periodically review the financial and operational condition of the service provider to assess its ability to continue to meet its outsourcing of IT Services obligation. The Bank would adopt risk-based approach in defining the periodicity. Such due diligence reviews would highlight any deterioration or breach in performance standards, confidentiality and security and in operational resilience preparedness.
- v) Operational Risk team should ensure to pro-actively intimate RBI through Compliance department, after ORMC/ RMCB declaration, of any adverse developments or non-compliance with legal and regulatory requirements in an outsourcing arrangement.
- vi) Board members, committees of the Board members, and senior management of IT functions would ensure oversight on outsourced IT services , which mainly covers the criteria for selection of such activities as well as service providers, parameters for defining material outsourcing based on the broad criteria, delegation of authority depending on risk and materiality, disaster recovery and business continuity plans, systems to monitor and review the operations of these activities and termination processes and exit strategies, including business continuity in the event of a third-party service provider exiting the outsourcing arrangement.

11.2 Service level agreements and performance metrics

The owner department should ensure to include SLAs in the outsourcing contracts to agree and establish accountability for performance expectations. SLAs must clearly formalize the performance criteria to measure the quality and quantity of service levels. The owner department, with support from Legal department of the Bank, should arrange to develop the following towards establishing an effective oversight program:

- i) Formal policy that defines the SLA program.
- ii) SLA monitoring process.
- iii) Recourse in case of non-performance.
- iv) Escalation process.
- v) Dispute resolution process.
- vi) Conditions in which the contract may be terminated by either party.

11.3 Measuring by key performance indicators (KPIs)

Bank would develop certain performance indicators under both normal and contingency circumstances for the services provided by the Service Provider and would assess the performance based on those indicators. Frequency of the assessment would also be allocated to each of the indicators for better management. Provisions need to be in place for timely and orderly intervention and rectification in the event of substandard performance by the service provider. The KPIs would mainly cover the service quality aspects, timely report submission by the service provider etc. The results of the KPIs would be shared with the Outsourcing Committee on an Annual basis for perusal and action required, if any.

Operations department would maintain record of all financial and technology outsourcing that is readily accessible for review by the Board and Senior Management of the Bank.

12. BUSINESS CONTINUITY AND MANAGEMENT OF DISASTER RECOVERY PLAN

The Operational Risk team of the Bank is required to establish a robust framework for documenting, maintaining and testing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) commensurate with the nature and scope of the outsourced activity as per extant instructions issued by RBI from time to time on BCP/ DR requirements.

Further, in establishing a viable contingency plan the Bank will consider the availability of alternative service providers or the possibility of bringing the outsourced activity back in-house in an emergency, and the costs, times and resources that would be involved.

In order to mitigate the risk of unexpected termination of the outsourcing agreement or insolvency/ liquidation of the service provider, the Bank will retain an appropriate level of control over their IT-outsourcing arrangement along with right to intervene, with appropriate measures to continue its business operations.

Outsourcing Committee should ensure that Bank's business continuity preparedness is not adversely compromised on account of outsourcing. Outsourcing Committee should adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.

- i) Department outsourcing critical activities should ensure that the activity happens in an uninterrupted way without causing any disruption to the Bank or its customers. Towards this end, concerned department should ensure the following before outsourcing.
- ii) Service providers have a good framework for documenting, maintaining, and testing business continuity and recovery procedures. Relevant departments may also conduct occasional joint testing and review the activities of service provider.
- iii) The relevant department should retain an appropriate level of control over their outsourcing and the right to intervene.
- iv) With appropriate measures to continue operations in unexpected scenarios, without incurring prohibitive expenses and without any break in the operations of the Bank and its services to the customers.
- v) The Outsourcing agreement should contain clauses for contingency plans and testing thereof, to maintain business continuity.
- vi) Outsourcing often leads to the sharing of facilities operated by the service provider. The Operational Risk team/Information Security/IT (Digital data records –IT, Data Security-IS) should ensure that service providers are able to isolate the bank's information, documents, and records and other assets. This is to ensure that in adverse conditions, all documents, records of transactions and information given to the service provider and assets of the bank can be removed from the possession of the service provider to continue its business operations, or deleted, destroyed, or rendered unusable.
- vii) Outsourcing Committee should ensure while framing the viable contingency plan, to consider the availability of alternative service providers or the possibility of bringing the outsourced activity back-in house in an emergency (for example, where number of vendors for a particular service is extremely limited) and the costs, time and resources that would be involved and take suitable preparatory action.

13. GRIEVANCES RELATING TO OUTSOURCED SERVICES

The Bank would ensure to constitute a Grievance redressal machinery within the bank and give wide publicity about it through electronic and print media.

Customers of the Bank can lodge a complaint against the service provider/ employee of the service provider through the customer grievance channel. The relevant department should maintain data of all such complaints and submit the same to the Outsourcing committee. The Outsourcing committee should factor in these complaints during their review.

Below are few points that must be included in Grievance redressal machinery:

- i) The name and contact number of designated grievance redressal officer of the Bank should be made known and widely publicized. The designated officer should ensure that genuine grievances of customers are redressed promptly without involving delay. It should be clearly indicated that the Bank's grievance redressal machinery will also deal with the issue relating to services provided by the outsourced agency.
- ii) A time limit of 30 days may be given to the customers for preferring their complaints/ grievances. The grievance redressal procedure of the Bank and the time frame fixed for responding to the complaints should be displayed on the Bank's website.
- iii) If a complainant does not get satisfactory response from the Bank within one month from the date of his/her lodging the complaint with the Bank, he/she will have the option to approach the Office of the concerned Banking Ombudsman for redressal of his/her grievance/s.

14. RISK EVALUATION AND MEASUREMENT

Risk evaluation would be performed prior to entering into an outsourcing agreement and reviewed periodically in the light of known and expected changes as part of the strategic planning or review processes. The Risk Evaluation should be done as per the established Outsourcing Policy/Process.

14.1 Framework for risk evaluation

Risk department would ensure a Risk Management Framework for outsourcing of IT services which shall comprehensively deal with the processes and responsibilities for identification, measurement, mitigation, management, and reporting of risks associated with Outsourcing of IT Services arrangements.

- i) Identification of role of outsourcing in the overall business strategy and objectives and inter-linkages with corporate strategic goals.
- ii) Analysis of impact of such arrangement on the overall risk profile of the bank and whether adequate internal expertise and resources exist to mitigate the risks identified.
- iii) Analysis of risk-return on the potential benefits of outsourcing vis-à-vis the vulnerabilities that may arise. Banks should evaluate vendor managed processes or specific vendor relationships as they relate to information systems and technology. All outsourced information systems and operations may be subject to risk management and security and privacy policies that meet the Bank's own standards.

- iv) The Risk Department and IT Department shall be responsible for the confidentiality and integrity of data and information pertaining to the customers that is available to the Service Provider.
- v) Public confidence and customer trust in Banks are a prerequisite for their stability and reputation. Hence, Risk Department / IT Department would seek to ensure the preservation and protection of the security and confidentiality of customer information in the custody or possession of the Service Provider. Access to customer information by staff of the Service Provider shall be on need-to-know basis.
- vi) In the event of multiple Service Provider relationships where two or more Service Providers collaborate to deliver an end-to-end solution, the Risk Department and IT Department remains responsible for understanding and monitoring the control environment of all service providers that have access to the Bank's data, systems, records or resources.
- vii) In instances where Service Provider acts as an outsourcing agent for multiple Banks, care shall be taken to build adequate safeguards so that there is no combining of information, documents, records and assets.
- viii) The Risk Department and IT Department would ensure that cyber incidents are reported to the Bank by the Service Provider without undue delay, so that the incident is reported by the Bank to the RBI within 6 hours of detection by the TPSP.
- ix) The Risk Department and IT Department would review and monitor the control processes and security practices of the Service Provider to disclose security breaches. The Risk Department and IT Department shall immediately notify RBI in the event of breach of security and leakage of confidential customer related information. In these eventualities, all the stakeholder of the Bank shall adhere to the extant instructions issued by RBI from time to time on Incident Response and Recovery Management.

14.2 Area of risk evaluation

Before deciding on outsourcing any service, Head-Operational Risk (Head-OR), CISO and the respective functional heads shall evaluate the risks associated with the activities to be outsourced and consider the same for outsourcing only if the risks are acceptable. The respective functional heads along with Head-OR/CISO shall identify and implement mitigation plan for all the high & medium risks being accepted and suggest suitable mitigates:

- a) **Strategic Risk** - Service provider may conduct the business on its own behalf, which may be inconsistent with the overall strategic goals of the Bank.
- b) **Reputation Risk** - Poor quality of service and customer interaction by service provider may not be as per the standards of the Bank.
- c) **Compliance Risk** - Privacy, Consumer and Prudential laws may not be adequately complied by the service provider.
- d) **Operational Risk** - Technical failures, fraud, errors, inadequate financial capability of service provider to meet obligations/provide remedies may cause such risks.

- e) **Legal Risk**- Exposure to fines, Penalties, or Punitive damages resulting from supervisory actions as well as private settlements due to omissions and commissions of the service provider etc.
- f) **Exit Strategy Risk** - This may arise from over-reliance on one firm, loss of relevant skills in the Bank itself might prevent it from bringing the activity back in-house.
- g) **Counter party Risk** - Due to inappropriate underwriting or credit assessments.
- h) **Country Risk** - Due to political, social or legal climate creating added risk.
- i) **Contractual Risk** - It may arise due to circumstantial difficulty in enforcing a contract.
- j) **Concentration and Systemic Risk** - It may arise when a number of Banks have considerable exposure to one service provider.

15. PERIODIC RISK ASSESSMENT, AUDIT AND REVIEWS

Operational Risk team should ensure to conduct pre and post outsourcing implementation reviews and also review its outsourcing arrangements periodically to ensure that its outsourcing risk management policies, procedures and guidelines are effectively complied with. The risk assessment carried out by the Bank is required to be documented along with necessary approvals. Such risk assessments are subject to annual internal and external quality assurance.

Information Security team should periodically review the independent audit and expert assessments on the security and control environment of the service provider, such assessments and reports on the service provider will be performed and prepared by the Bank's internal or external auditors or by agents appointed by the Bank. The findings of the audit activity to be presented to the Outsourcing Committee. The Bank will be responsible for the confidentiality and integrity of data and information pertaining to customers that is available to service provider.

Such reviews should take adequate cognizance of historical violations or issue remediation during previous audits and assessments. Copies of previous audits and assessments should be shared during RBI inspections.

Access to data at the Bank's location/ data centre by service providers would be on need-to-know basis, with appropriate controls to prevent security breaches and/ or data misuse.

15.1 Review of outsourcing arrangements

Outsourcing Committee would review the financial and operational condition of the service provider to assess its ability to continue to meet outsourcing obligations. Such due diligence reviews, which can be based on all available information about the service provider including reports by the service provider's external auditors. Any deterioration or breach in performance standards, confidentiality and security and its business continuity preparedness should be highlighted in the review.

Outsourcing Committee should carry out Annual review of all outsourcing arrangements as per the contract date.

The review report along with the observations & action taken should be submitted to the subsequent Risk Management Committee of the Board.

Half Yearly Review (Off-site) - A half yearly review of the operational risk associated with the services provided shall be undertaken by the department of the Bank responsible for onboarding of the vendor in order to assess its ability to continue to meet its outsourcing obligation. This review would be based on the checklist and self-certification by the Service Provider. A report on the findings of the review undertaken by the concerned department of the Bank will be put up to Operational Risk (OR) team prior to submission to the Outsourcing Committee of the Bank and the respective departmental heads to whom the function is outsourced for perusal and action required, if any.

Annual Review (On-site) – The department responsible for Outsourcing the activity of the Bank should conduct the on-site review of the activities provided by the Service Provider to ensure all parameters largely viz, performance, financial stability, BCP standards and Data Security standards. The review would be based on the half yearly submission report provided to the bank by the vendor/Service provider. Report on the findings of the review undertaken by the officer of the Bank should be put up to the OR team prior to submission to the Outsourcing Committee of the Bank and to the respective departments to whom the function is outsourced for perusal and action required.

Note: Any vendor that falls under High Risk category post their Risk Scoring by Operational Risk team based on the information provided in the Risk Assessment Format (Annexure 1) by the vendor during half yearly review, the onsite visit will be done by the Risk team on a case-to-case basis as may be deemed fit.

16. OTHER MANDATORY REGULATORY REQUIREMENTS

Following regulatory requirements are to be fulfilled by the relevant departments before outsourcing an activity to the service provider:


- i) Service Provider should seek prior approval of the Bank (relevant department, outsourcing the activity) for use of sub-contractors for all or any part of the outsourced activity. The relevant department should ensure that the sub-contracting arrangements are compliant with the extant regulatory guidelines on outsourcing.
- ii) In cases like outsourcing of cash management services, involving reconciliation of transactions, service provider/sub-contractor should ensure that reconciliation of transactions between the Bank and service provider (and/ or its subcontractor) are carried out in a timely manner.
- iii) An ageing analysis of such entries pending reconciliation with outsourced service providers should be placed before the Audit Committee of the Board (ACB).
- iv) Internal audit department should conduct an audit of outsourced activities and submit the report to ACB.
- v) Internal audit department would submit an 'Annual Compliance Certificate' giving particulars of outsourcing contracts, periodicity of audit by internal/ external auditor, major findings of the audit and action taken through Board, to the Chief General Manager in-Charge, Department of Banking Supervision, Central Office, Reserve Bank of India, Mumbai.
- vi) All products literature/ brochures etc. should have a clause stating that Bank may use the services of agents in sales/ marketing etc., of the products. The role of agents, if any should also be indicated in broad terms.

17. REPORTING TO INDIAN BANKS ASSOCIATION

Outsourcing Committee should ensure reporting of required information to below authority:

Indian Banks Association (IBA) – All cases for ‘termination for cause’ have to be reported by concerned departments to Outsourcing committee and Outsourcing committee shall intimate to Compliance department for inclusion in IBA caution list.

Annexure:

Sr. No.	Name of Annexure	Attachment
1.	Annexure 1 Risk Assessment Format	 Annexure 1.xlsx

Appendix – I
Usage of Cloud Computing Services

Cloud Policy is a part of Bank’s IT Policy where selection and implementation of cloud technology and service providers are given. The security aspects, management, disaster management, exit strategy etc. are a part of Bank’s IS Policy.

Appendix – II
Outsourcing of Security Operations Centre

Outsourcing of Security Operations Centre (SOC) operations has the risk of data being stored and processed at an external location and managed by a third party (Managed Security Service Provider (MSSP)) to which Bank have lesser visibility. To mitigate the risks, in addition to the controls prescribed in these Directions, Bank would adopt the following requirements in the case of outsourcing of SOC operations:

- i) unambiguously identify the owner of assets used in providing the services (systems, software, source code, processes, concepts, etc.);
- ii) ensure that the Bank has adequate oversight and ownership over the rule definition, customisation and related data/ logs, meta-data and analytics (specific to the Bank);
- iii) assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically;
- iv) integrate the outsourced SOC reporting and escalation process with the Bank’s incident response process; and
- v) review the process of handling of the alerts / events.

Appendix – III
Services not considered under Outsourcing of IT Services

A. Services / Activities not considered under “Outsourcing of IT Services” for the purpose of this Master Direction (an indicative but not exhaustive list)

- i) Corporate Internet Banking services obtained by regulated entities as corporate customers/ sub members of another regulated entity
- ii) SMS gateways (Bulk SMS service providers)
- iii) Procurement of IT hardware/ appliances

- iv) Applications provided by financial sector regulators or institutions like CCIL, NSE, BSE, etc.
- v) Platforms provided by entities like Reuters, Bloomberg, SWIFT, etc.
- vi) Any other off the shelf products (like anti-virus software, email solution, etc.,) subscribed to by the regulated entity wherein only a license is procured with no/ minimal customisation
- vii) Services obtained by a Bank as a sub-member of a Centralised Payment Systems (CPS) from another Bank.

B. Vendors / Entities who are not considered as Third-Party Service Provider for the purpose of this Master Direction (an indicative but not exhaustive list)

- i) Vendors providing business services using IT. Example – BCs
- ii) Payment System Operators authorised by the Reserve Bank of India under the Payment and Settlement Systems Act, 2007 for setting up and operating Payment Systems in India
- iii) Partnership based Fintech firms such as those providing co-branded applications, service, products (would be considered under outsourcing of financial services)
- iv) Services of Fintech firms for data retrieval, data validation and verification services such as (list is not exhaustive):
 - a) Bank statement analysis
 - b) GST returns analysis
 - c) Fetching of vehicle information
 - d) Digital document execution
 - e) Data entry and Call centre services
- v) Telecom Service Providers from whom leased lines or other similar kind of infrastructure are availed and used for transmission of the data
- vi) Security/ Audit Consultants appointed for certification/ audit/ VA-PT related to IT infra/ IT services/ Information Security services in their role as independent third-party auditor/ consultant/ lead implementer.