AGREEMENT FOR SUPPORT FOR INFRASTRUCTURE AND SERVICES OF APPLICATIONS OF FOREIGN OFFICES (FO) OF SBI FOR PERIOD OF THREE YEARS[1]

BETWEEN

STATE BANK OF INDIA

IT-FOREIGN OFFICES DEPARTMENT

AND

_____[2]

Date of Commencement : _____

Date of Expiry : _____

[1] Type/nature/name of Agreement.
2 The other Party (Contractor/ Service Provider) to the Agreement

Table of contents

This agreement ("Agreement") is made at_____ (Place) on this _____day of _____ 20__.

BETWEEN

State Bank of India, constituted under the State Bank of India Act, 1955 having its Corporate Centre at State Bank Bhavan, Madame Cama Road, Nariman Point, Mumbai-21 and its Global IT Centre at Sector-11, CBD Belapur, Navi Mumbai- 400614 through its IT-RRBs & FO Tech Ops, State Bank Global IT Centre, Kapas Bhawan, 3rd Floor, Nirmala Devi Marg, Sector-10,CBD Belapur, Navi Mumbai, Maharashtra, India 400614, hereinafter referred to as "**the Bank**" which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors in title and assigns of First Part:

AND

_____[3] a private/public limited company/LLP/Firm incorporated under the provisions of the Companies Act, 1956/ Limited Liability Partnership Act 2008/ Indian Partnership Act 1932, having its registered office at _____ hereinafter referred to as "**Service Provider/ Vendor**", which expression shall mean to include its successors in title and permitted assigns of the Second Part:

WHEREAS

(i) "The Bank" is carrying on business in banking in India and overseas and desirous to avail services for infrastructure managed services and services of applications of Foreign Offices (FOs) of SBI.

(ii) Service Provider is in the business of providing _____ and has agreed to provide the services as may be required by the Bank mentioned in the Request of Proposal (RFP) No. SBI/GITC/ITFO/2022/2023/887 dated 19.09.2022 issued by the Bank along with its clarifications/ corrigenda, referred hereinafter as a "RFP" and same shall be part of this Agreement.

3Name & Complete Address (REGISTERED OFFICE) of service Provider,

NOW THEREFORE, in consideration of the mutual covenants, undertakings and conditions set forth below, and for other valid consideration the acceptability and sufficiency of which are hereby acknowledged, the Parties hereby agree to the following terms and conditions hereinafter contained:-

1. DEFINITIONS & INTERPRETATION

1.1 Definition

Certain terms used in this Agreement are defined hereunder. Other terms used in this Agreement are defined where they are used and have the meanings there indicated. Unless otherwise specifically defined, those terms, acronyms and phrases in this Agreement that are utilized in the information technology services industry or other pertinent business context shall be interpreted in accordance with their generally understood meaning in such industry or business context, unless the context otherwise requires/mentions, the following definitions shall apply:

1.1.1 'The Bank' shall mean State Bank of India (including domestic branches and foreign offices), Subsidiaries and Joint Ventures, where the Bank has ownership of more than 50% of voting securities or the power to direct the management and policies of such Subsidiaries and Joint Ventures.

1.1.2 "Confidential Information" shall have the meaning set forth in Clause 14.

1.1.3 Data Dictionary or Metadata Repository" shall mean a repository of information about data such as meaning, relationships to other data, origin/lineage, usage, business context and format including but not limited to data type, data length, data structure etc., further, it as a collection of columns and tables with metadata.

1.1.4 "Deficiencies" shall mean defects arising from non-conformity with the mutually agreed specifications and/or failure or non-conformity in the Scope of the Services.

1.1.5 "Documentation" will describe in detail and in a completely self-contained manner how the User may access and manage the support for infrastructure and services of applications of Foreign Offices (FO) of SBI such that any reader of the Documentation can access, use and maintain all of the functionalities of the above engagement without the need for any further instructions. 'Documentation' includes, user manuals, installation manuals, operation manuals, design documents, process documents, data flow documents, data register, technical manuals, functional specification, software

requirement specification, on-line tutorials/CBTs, system configuration documents, Data Dictionary, system/database administrative documents, debugging/diagnostics documents, test procedures, Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all Product components, list of all dependent/external modules and list of all documents relating to traceability of the Product as and when applicable etc.

1.1.6 "Intellectual Property Rights" shall mean, on a worldwide basis, any and all: (a) rights associated with works of authorship, including copyrights &moral rights; (b) Trade Marks; (c) trade secret rights; (d) patents, designs, algorithms and other industrial property rights; (e) other intellectual and industrial property rights of every kind and nature, however designated, whether arising by operation of law, contract, license or otherwise; and (f) registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing).

1.1.7 "Project Cost" means the price payable to Service Provider over the entire period of Agreement (i.e. Rs._____<*in words*>) for the full and proper performance of its contractual obligations.

1.1.8 "Request for Proposal (RFP)" shall mean RFP NO. SBI/GITC/ITFO/2022/2023/887 dated 19.09.2022 along with its clarifications/ corrigenda issued by the Bank time to time.

1.1.9 "Root Cause Analysis Report" shall mean a report addressing a problem or non-conformance, in order to get to the 'root cause' of the problem, which thereby assists in correcting or eliminating the cause, and prevent the problem from recurring.

1.1.10 'Services' shall mean and include the Services offered by Service Provider under this Agreement more particularly described in Clause 2 of this Agreement.

1.2 **Interpretations:**

1.2.1 Reference to a person includes any individual, firm, body corporate, association (whether incorporated or not) and authority or agency (whether government, semi government or local).

1.2.2 The singular includes the plural and vice versa.

1.2.3 Reference to any gender includes each other gender.

1.2.4 The provisions of the contents table, headings, clause numbers, italics, bold print and underlining is for ease of reference only and shall not affect the interpretation of this Agreement.

1.2.5 The Schedules, Annexures and Appendices to this Agreement shall form part of this Agreement.

1.2.6 A reference to any documents or agreements (and, where applicable, any of their respective provisions) means those documents or agreements as amended, supplemented or replaced from time to time provided they are amended, supplemented or replaced in the manner envisaged in the relevant documents or agreements.

1.2.7 A reference to any statute, regulation, rule or other legislative provision includes any amendment to the statutory modification or re-enactment or, legislative provisions substituted for, and any statutory instrument issued under that statute, regulation, rule or other legislative provision.

1.2.8 Any agreement, notice, consent, approval, disclosure or communication under or pursuant to this Agreement is to be in writing.

1.2.9 The terms not defined in this agreement shall be given the same meaning as given to them in the RFP. If no such meaning is given technical words shall be understood in technical sense in accordance with the industrial practices.

1.3 Commencement, Term & Change in Terms

1.3.1 This Agreement shall commence from its date of execution mentioned above/ be deemed to have commenced from _____ (Effective Date).

1.3.2 This Agreement shall be in force for a period of 3 year(s) from Effective Date, unless terminated by the Bank by notice in writing in accordance with the termination clauses of this Agreement.

1.3.3 The Bank shall have the right at its discretion to renew this Agreement in writing, for a further term of 2 years on the mutually agreed terms & conditions.

2. SCOPE OF WORK

2.1 The scope and nature of the work which Service Provider has to provide to the Bank (Services) is described in **Annexure-A.**

2.2 The Bank may, at its sole discretion, provide remote access to its information technology system to IT Service Provider through secured Virtual Private Network (VPN) in order to facilitate the performance of IT Services. Such remote access to the Bank's information technology system shall be subject to the following:

2.1.1 Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.

2.1.2 Service Provider shall ensure that only its authorized employees/representatives access the Device.

2.1.3 Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.

2.1.4 Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.

2.1.5 Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. Service Provider shall facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.

2.1.6 Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure the Bank's information technology system is not compromised in the course of using remote access facility.

3. FEES /COMPENSATION

3.1 Professional fees

3.1.1 Service Provider shall be paid fees and charges in the manner detailed in here under, the same shall be subject to deduction of income tax thereon wherever required under the provisions of the Income Tax Act by the Bank. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by the Bank as per the laws and regulations for the time being in force. Nothing in the Agreement shall relieve Service Provider from his responsibility to pay any tax that may be levied in India on income and profits made by Service Provider in respect of this Agreement.

3.2 All duties and taxes (excluding GST or any other tax imposed by the Government in lieu of same), if any, which may be levied, shall be borne by Service Provider and Bank shall not be liable for the same. All expenses, stamp duty and other charges/ expenses in connection with execution of this Agreement shall be borne by Service Provider. GST or any other tax imposed by the Government in lieu of same shall be borne by the Bank on actual upon production of original receipt wherever required.

3.3 Service Provider shall provide a clear description quantifying the service element and goods element in the invoices generated by them.

3.4 Payments

3.4.1 The Bank will pay properly submitted valid invoices within reasonable period but not exceeding 30 (thirty) days after its receipt thereof. All payments shall be made in Indian Rupees.

3.4.2 The Bank may withhold payment of any product/services that it disputes in good faith and may set-off penalty amount or any other amount which Service Provider owes to the Bank against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, the Bank shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidences, if any, within 21 (twenty one) days. Penalty or damages, if any, recoverable from Service Provider shall be recovered by the Bank through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised

invoice, the Bank shall have right to withhold the payment or set-off penal amount from current invoices.

3.5 Bank Guarantee and Penalties

3.5.1 Service Provider shall furnish performance security in the form of Bank Guarantee for an amount equivalent rupees of 3 % of the contract amount valid for a period of 3 years 3 months from a Scheduled Commercial Bank other than State Bank of India in a format provided/ approved by the Bank.

3.5.2 The Bank Guarantee is required to protect the interest of the Bank against the risk of non-performance of Service Provider in respect of successful implementation of the project and/or failing to perform / fulfil its commitments / obligations in respect of providing Services as mentioned in this Agreement; or breach of any terms and conditions of the Agreement, which may warrant invoking of Bank Guarantee.

3.5.3 If at any time during performance of the contract, Service Provider shall encounter unexpected conditions impeding timely completion of the Services under the Agreement and performance of the services, Service Provider shall promptly notify the Bank in writing of the fact of the delay, it's likely duration and its cause(s). As soon as practicable, after receipt of Service Provider's notice, the Bank shall evaluate the situation and may at its discretion extend Service Provider's time for performance, in which case the extension shall be ratified by the Parties by amendment of the Agreement.

3.5.4 Performance of the obligations under the Agreement shall be made by Service Provider in accordance with the time schedule[4] specified in this Agreement.

3.5.5 Service Provider shall be liable to pay penalty at the rate mentioned in **Annexure-E** in respect of any delay beyond the permitted period in providing the Services.

3.5.6 No penalty shall be levied in case of delay(s) in deliverables or performance of the contract for the reasons solely and directly attributable to the Bank. On reaching the maximum of penalties specified the Bank reserves the right to terminate the contract.

[4] Please ensure that the time scheduled is suitably incorporated in the Agreement.

4. LIABILITIES/OBLIGATION

4.1 The Bank's Duties /Responsibility(if any)

(i) Processing and authorising invoices

(ii) Provision of access to Data Centre

(iii) The Bank will provide workstation, desktop and software reasonably required for service provider's resources to perform the services on site at the Bank's facilities.

4.2 Service Provider Duties

(i) Service Delivery responsibilities

(a) To adhere to the service levels documented in this Agreement.

(b) Service Provider shall ensure to filter all phishing / spamming / overflow attacks in order to ensure availability and integrity on continuous basis.

(c) Service Provider shall ensure that Service Provider's personnel and its sub-contractors (if allowed) will abide by all reasonable directives issued by the Bank, including those set forth in the Bank's then-current standards, policies and procedures (to the extent applicable), all on-site rules of behaviour, work schedules, security procedures and other standards, policies and procedures as established by the Bank from time to time.

(d) Service Provider agrees and declares that it shall be the sole responsibility of Service Provider to comply with the provisions of all the applicable laws, concerning or in relation to rendering of Services by Service Provider as envisaged under this Agreement.

(e) Service Provider shall be responsible to provide Data Dictionary in a format provided by the Bank. During the term of this Agreement, such a format may be revised by the Bank as per the requirements. Service Provider shall capture all the fields in Data Dictionary format and keep the same always updated during the term of this Agreement.

(ii) Security Responsibility

a) To maintain the confidentiality of the Bank's resources and other intellectual property rights.

(b) Service Provider shall have to comply with Bank's IT & IS Security policy in key concern areas relevant to the Agreement, details of which will be shared with the Service Provider. Some of the key areas are as under:

i. Responsibilities for data and application privacy and confidentiality.

ii. Responsibilities on system and software access control and administration.

iii. Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to Service Provider.

iv. Physical Security of the facilities.

v. Physical and logical separation from other customers of Service Provider.

vi. Incident response and reporting procedures.

vii. Password Policy of the Bank.

viii. Data Encryption/Protection requirements of the Bank.

ix. In general, confidentiality, integrity and availability must be ensured.

(iii) To comply with other obligations and responsibilities as defined under this agreement.

(iv) Service provider shall comply with the provision of GDPR.

5. REPRESENTATIONS &WARRANTIES

5.1 Each of the Parties represents and warrants in relation to itself to the other that:

5.1.1 It has all requisite corporate power and authority to execute, deliver and perform its obligations under this Agreement and has been fully authorized through applicable corporate process to do so.

5.1.2 The person(s) signing this Agreement on behalf of the Parties have the necessary authority and approval for execution of this document and to bind his/their respective organization for due performance as set out in this Agreement. It has all necessary statutory and regulatory permissions, approvals and permits for the running and operation of its business.

5.1.3 It has full right, title and interest in and to all software, copyrights, trade names, trademarks, service marks, logos symbols and other proprietary marks (collectively 'IPR') (including appropriate limited right of use of those owned by any of its vendors, affiliates or subcontractors) which it provides to the other Party, for use related to the Services to be provided under this Agreement.

5.1.4 It will provide such cooperation as the other Party reasonably requests in order to give full effect to the provisions of this Agreement.

5.1.5 The execution and performance of this Agreement by either of the Parties does not and shall not violate any provision of any of the existing Agreement with any of the party and any other third party.

5.2 **Additional Representation and Warranties by Service Provider**

5.2.1 Service Provider shall perform the Services and carry out its obligations under the Agreement with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and with professional standards recognized by international professional bodies and shall observe sound management practices. It shall employ appropriate advanced technology and safe and effective equipment, machinery, material and methods.

5.2.2 Service Provider has the requisite technical and other competence, sufficient, suitable, qualified and experienced manpower/personnel and expertise in providing the Services to the Bank.

5.2.3 Service Provider shall duly intimate to the Bank immediately, the changes, if any in the constitution of Service Provider.

5.2.4 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the services and products provided by Service Provider to the Bank do not violate or infringe any patent, copyright, trademarks, trade secrets or other intellectual property rights of any third party.

5.2.5 Service provider shall ensure that all persons, employees, workers and other individuals engaged by or sub-contracted (if allowed) by Service Provider in rendering the Services under this Agreement have undergone proper background check, police verification and other necessary due diligence checks to examine their antecedence and ensure their suitability for such engagement. No person shall be engaged by Service provider unless such person is found to be suitable in such verification and Service Provider shall retain the records of such verification and shall produce the same to the Bank as and when requested.

5.2.6 Service Provider warrants that at the time of delivery the software deployed/ upgraded as a part of this Agreement is free from malware, free from any obvious bugs, and free from any covert channels in the code (of the versions of the applications/software being delivered as well as any subsequent versions/modifications done). Software deployed/ upgraded as a part of this Agreement shall remain free from OWASP Top 10 vulnerabilities (latest) during the term of this Agreement.

5.2.7 Service Provider represents and warrants that its personnel shall be present at the Bank premises or any other place as the bank may direct, only for the Services and follow all the instructions provided by the Bank; act diligently, professionally and shall maintain the decorum and environment of the Bank; comply with all occupational, health or safety policies of the Bank.

5.2.8 Service Provider warrants that it shall be solely liable and responsible for compliance of applicable Labour Laws in respect of its employee, agents, representatives and sub-contractors (if allowed) and in particular laws relating to terminal benefits such as pension, gratuity, provident fund, bonus or other benefits to which they may be entitled and the laws relating to contract labour, minimum wages, etc., and the Bank shall have no liability in this regard.

5.2.9 During the Contract period, if any software or any component thereof is supplied by Service Provider is inoperable or suffers degraded performance, Service provider shall, at the Bank's request, promptly replace the software or specified component with new software of the same type and quality. Such replacement shall be accomplished without any adverse impact on the Bank's operations within agreed time frame and without any additional cost to the Bank.

6. GENERAL INDEMNITY

6.1 Service Provider agrees and hereby keeps the Bank indemnified against all claims, actions, loss, damages,, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which the Bank may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any wilful misconduct and gross negligent acts on the part of employees, agents, representatives or sub-contractors (if allowed) of Service Provider. Service Provider agrees to make good the loss suffered by the Bank.

6.2 Service Provider hereby undertakes the responsibility to take all possible measures, at no additional cost, to avoid or rectify any issues which thereby results in non-performance of software/ hardware/ deliverables within reasonable time. The Bank shall report as far as possible all material defects to Service Provider without undue delay. Service Provider also undertakes to co-operate with other service providers thereby ensuring expected performance covered under scope of work.

7. CONTINGENCY PLANS

Service Provider shall arrange and ensure proper data recovery mechanism, attrition plan and other contingency plans to meet any unexpected obstruction to Service Provider or any employees or sub-contractors (if allowed) of Service Provider in rendering the Services or any part of the same under this Agreement to the Bank. Service Provider at Banks discretion shall co-operate with the Bank in case on any contingency.

8. TRANSITION REQUIREMENT

In the event of failure of Service Provider to render the Services or in the event of termination of Agreement or expiry of term or otherwise, without prejudice to any other right, the Bank at its sole discretion may make alternate arrangement for getting the Services contracted with another vendor. In such case, the Bank shall give prior notice to the existing Service Provider. The existing Service Provider shall continue to provide services as per the terms of the Agreement until a 'New Service Provider' completely takes over the work. During the transition phase, the existing Service Provider shall render all reasonable assistances to the new Service Provider within such period prescribed by the Bank, at no extra cost to the Bank, for ensuring smooth switch over and continuity of Services, provided where transition services are required by the Bank or New Service Provider beyond the term of this Agreement, reasons for which are not attributable to Service Provider, payment shall be made to Service Provider for such additional period on the same rates and payment terms as specified in this Agreement. If existing vendor is found to be in breach of this obligation, they shall be liable for paying a penalty as mentioned in this Annexure-E on demand to the Bank, which may be settled from the payment of invoices or bank guarantee for the contracted period. Transition & Knowledge Transfer plan is mentioned in Annexure F.

9. LIQUIDATED DAMAGES

If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this Agreement, the Bank may, without prejudice to its other remedies under the Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5 % of total Project cost for delay of each week or part thereof maximum up to 5 % of total Project cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.

10. RELATIONSHIP BETWEEN THE PARTIES

10.1 It is specifically agreed that Service Provider shall act as independent service provider and shall not be deemed to be the Agent of the Bank except in respect of the transactions/services which give rise to Principal - Agent relationship by express agreement between the Parties.

10.2 Neither Service Provider nor its employees, agents, representatives, Sub-Contractors shall hold out or represent as agents of the Bank.

10.3 None of the employees, representatives or agents of Service Provider shall be entitled to claim any absorption or any other claim or benefit against the Bank.

10.4 This Agreement shall not be construed as joint venture. Each Party shall be responsible for all its obligations towards its respective employees. No employee of any of the two Parties shall claim to be employee of other Party.

10.5 All the obligations towards the employee(s) of a Party on account of personal accidents while working in the premises of the other Party shall remain with the respective employer and not on the Party in whose premises the accident occurred unless such accidents occurred due to gross negligent act of the Party in whose premises the accident occurred.

10.6 For redressal of complaints of sexual harassment at workplace, Parties agree to comply with the policy framed by the Bank (including any amendment thereto) in pursuant to the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 including any amendment thereto.

11. SUB CONTRACTING

As per the scope of this Agreement sub-contracting is not permitted.

12. INTELLECTUAL PROPERTY RIGHTS

12.1 For any technology / software / product used/supplied by Service Provider for performing Services for the Bank as part of this Agreement, Service Provider shall have right to use as well as right to license such technology/ software / product. The Bank shall not be liable for any license or IPR violation on the part of Service Provider.

12.2 Without the Bank's prior written approval, Service provider will not, in performing the Services, use or incorporate link to or call or depend in any way upon, any software or other intellectual property that is subject to an Open Source or Copy left license or any other agreement that may give rise to any third-party claims or to limit the Bank's rights under this Agreement.

12.3 Subject to clause 12.4 and 12.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the

Bank against all costs, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from the Services or use of the technology / software / products or any part thereof in India or abroad.

12.4 The Bank will give (a) notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; (b) sole authority to defend and settle such claim and; (c) will at no time admit to any liability for or express any intent to settle the claim provided that (i) Service Provider shall not partially settle any such claim without the written consent of the Bank, unless such settlement releases the Bank fully from such claim, (ii) Service Provider shall promptly provide the Bank with copies of all pleadings or similar documents relating to any such claim, (iii) Service Provider shall consult with the Bank with respect to the defense and settlement of any such claim, and (iv) in any litigation to which the Bank is also a party, the Bank shall be entitled to be separately represented at its own expenses by counsel of its own selection.

12.5 Service Provider shall have no obligations with respect to any infringement claims to the extent that the infringement claim arises or results from: (i) Service Provider's compliance with the Bank's specific technical designs or instructions (except where Service Provider knew or should have known that such compliance was likely to result in an Infringement Claim and Service Provider did not inform the Bank of the same); or (ii) any unauthorized modification or alteration of the deliverable (if any) by the Bank.

13. INSPECTION AND AUDIT

13.1 It is agreed by and between the parties that Service Provider shall be subject to annual audit by internal/external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to the Bank and Service Provider shall submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by Service Provider. Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7

(seven) days to Service Provider before such audit and same shall be conducted during normal business hours.

13.2 Where any Deficiency has been observed during audit of Service Provider on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, it is agreed upon by Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the Deficiencies. It is also agreed that Service Provider shall provide certification of the auditor to the Bank regarding compliance of the observations made by the auditors covering the respective risk parameters against which such Deficiencies observed.

13.3 Service Provider further agrees that whenever required by the Bank, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the Bank/ Reserve Bank of India and/or any regulatory authority (ies). The Bank reserves the right to call for and/or retain any relevant information / audit reports on financial and security reviews with their findings undertaken by Service Provider. However, Service Provider shall not be obligated to provide records/ data not related to Services under the Agreement (e.g. internal cost breakup etc.).

14. CONFIDENTIALITY

14.1 "Confidential Information" mean all information which is material to the business operations of either party or its affiliated companies, designated as being confidential or which, under the circumstances surrounding disclosure out to be treated as confidential, in any form including, but not limited to, proprietary information and trade secrets, whether or not protected under any patent, copy right or other intellectual property laws, in any oral, photographic or electronic form, whether contained on computer hard disks or floppy diskettes or otherwise without any limitation whatsoever. Without prejudice to the generality of the foregoing, the Confidential Information shall include all information about the party and its customers, costing and technical data, studies, consultants reports, financial information, computer models and programs, software Code, contracts, drawings, blue prints, specifications, operating techniques, processes, models, diagrams, data sheets, reports and other information with respect to any of the foregoing matters. All and every information received by the parties and marked confidential hereto shall be assumed to be confidential information unless otherwise proved. It is further agreed that the information relating to the Bank and its customers is deemed confidential whether marked confidential or not.

14.2 All information relating to the accounts of the Bank's customers shall be confidential information, whether labeled as such or otherwise.

14.3 All information relating to the infrastructure and Applications (including designs and processes) shall be deemed to be Confidential Information whether labeled as such or not. Service Provider personnel/resources responsible for the project are expected to take care that their representatives, where necessary, have executed a Non-Disclosure Agreement similar to comply with the confidential obligations under this Agreement.

14.4 Each party agrees that it will not disclose any Confidential Information received from the other to any third parties under any circumstances without the prior written consent of the other party unless such disclosure of Confidential Information is required by law, legal process or any order of any government authority. Service Provider in this connection, agrees to abide by the laws especially applicable to confidentiality of information relating to customers of Banks and the banks per-se, even when the disclosure is required under the law. In such event, the Party must notify the other Party that such disclosure has been made in accordance with law; legal process or order of a government authority.

14.5 Each party, including its personnel, shall use the Confidential Information only for the purposes of achieving objectives set out in this Agreement. Use of the Confidential Information for any other purpose shall constitute breach of trust of the same.

14.6 Each party may disclose the Confidential Information to its personnel solely for the purpose of undertaking work directly related to the Agreement. The extent of Confidential Information disclosed shall be strictly limited to what is necessary for those particular personnel to perform his/her duties in connection with the Agreement. Further each Party shall ensure that each personnel representing the respective party agree to be bound by obligations of confidentiality no less restrictive than the terms of this Agreement.

14.7 The non-disclosure obligations herein contained shall not be applicable only under the following circumstances:

(i) Where Confidential Information comes into the public domain during or after the date of this Agreement otherwise than by disclosure by a receiving party in breach of the terms hereof.

(ii) Where any Confidential Information was disclosed after receiving the written consent of the disclosing party.

(iii) Where receiving party is requested or required by law or by any Court or governmental agency or authority to disclose any of the Confidential Information, then receiving party will provide the other Party with prompt notice of such request or requirement prior to such disclosure.

(iv) Where any Confidential Information was received by the receiving party from a third party which does not have any obligations of confidentiality to the other Party.

(v) Where Confidential Information is independently developed by receiving party without any reference to or use of disclosing party's Confidential Information.

14.8 Receiving party undertakes to promptly notify disclosing party in writing any breach of obligation of the Agreement by its employees or representatives including confidentiality obligations. Receiving party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies, to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction.

14.9 Service Provider shall not, without the Bank's prior written consent, make use of any document or information received from the Bank except for purposes of performing the services and obligations under this Agreement.

14.10 Any document received from the Bank shall remain the property of the Bank and shall be returned (in all copies) to the Bank on completion of Service Provider's performance under the Agreement.

14.11 Upon expiration or termination of the Agreement, all the Bank's proprietary documents, customized programs partially or wholly completed and associated documentation, or the Bank's materials which are directly related to any project under the Agreement shall be delivered to the Bank or at the Bank's written instruction destroyed, and no copies shall be retained by Service provider without the Bank's written consent.

14.12 The foregoing obligations (collectively referred to as "Confidentiality Obligations") set out in this Agreement shall survive the term of this Agreement and for a period of five (5) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer's data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.

15. OWNERSHIP

15.1 Service Provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all intellectual property rights, copyrights. Any work made under this Agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.

15.2 The Intellectual Property Rights on the software code, copyright and source code for various applications/ interfaces developed under this Agreement, and any other component/ framework/ middleware used/ developed as pre-built software assets to deliver the solution,

shall belong to the Bank and the Bank shall have complete and unrestricted rights on such property. However, Service Provider shall hold All Intellectual Property rights in any pre-built software *per se*, except for those which have been assigned under this Agreement.

15.3 All information processed by Service Provider during software maintenance belongs to the Bank. Service Provider shall not acquire any other right in respect of the information for the license to the rights owned by the Bank. Service Provider will implement mutually agreed controls to protect the information. Service Provider also agrees that it will protect the information appropriately.

16. TERMINATION

16.1 The Bank may, without prejudice to any other remedy for breach of Agreement, by written notice of not less than 30 (thirty) days, terminate the Agreement in whole or in part:

(i) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement, or any extension thereof granted by the Bank;

(ii) If Service Provider fails to perform any other obligation(s) under the Agreement;

(iii) Violations of any terms and conditions stipulated in the RFP;

(iv) On happening of any termination event mentioned herein above in this Agreement.

Prior to providing a written notice of termination to Service Provider under clause 16.1 (i) to 16.1 (iii), the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.

16.2 The Bank, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, for its convenience, provided same shall not be invoked by the Bank before completion of half of the total Contract period (including the notice period). In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.

16.3 In the event the Bank terminates the Agreement in whole or in part for the breaches attributable to Service Provider, the bank may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to clause 20 Service Provider shall be liable to the Bank for any increase in costs for such similar

Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement to the extent not terminated.

16.4 The Bank shall have a right to terminate the Agreement immediately by giving a notice in writing to Service Provider in the following eventualities:

(i) If any Receiver/Liquidator is appointed in connection with the business of Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider.

(ii) If Service Provider applies to the Court or passes a resolution for voluntary winding up of or any other creditor / person files a petition for winding up or dissolution of Service Provider.

(iii) If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors or representatives, in the reasonable opinion of the Bank tantamount to fraud or prejudicial to the interest of the Bank or its employees.

(iv) Any document, information, data or statement submitted by Service Provider in response to RFP, based on which Service Provider was considered eligible or successful, is found to be false, incorrect or misleading.

16.5 In the event of the termination of the Agreement Service Provider shall be liable and responsible to return to the Bank all records, documents, data and information including Confidential Information pertains to or relating to the Bank in its possession.

16.6 In the event of termination of the Agreement for material breach, the Bank shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations.

16.7 Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution clause; and any right which a Party may have under the applicable Law.

17. DISPUTE REDRESSAL MECHANISM & GOVERNING LAW

17.1 All disputes or differences whatsoever arising between the parties out of or in connection with this Agreement (including dispute concerning interpretation) or in discharge of any obligation arising out of the Agreement (whether during the progress of work or after completion of such work and whether before or after the termination of this Agreement, abandonment or breach of this Agreement), shall be settled amicably.

17.2 If the parties are not able to solve them amicably within 30 (thirty) days after dispute occurs as evidenced through the first written communication from any party notifying the other regarding the disputes, either party (the Bank or Service Provider) shall give written notice to other party clearly setting out there in, specific dispute(s) and/or difference(s), and shall be referred to a sole arbitrator mutually agreed upon, and the award made in pursuance thereof shall be binding on the parties.

17.3 In the absence of consensus about the single arbitrator, the dispute may be referred to an arbitration panel; one to be nominated by each party and the said arbitrators shall nominate a presiding arbitrator, before commencing the arbitration proceedings. The arbitration shall be settled in accordance with the applicable Indian Laws and the arbitration shall be conducted in accordance with the Arbitration and Conciliation Act, 1996.

17.4 Service Provider shall continue work under the Agreement during the arbitration proceedings, unless otherwise directed by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained.

17.5 Arbitration proceeding shall be held at **Mumbai**, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be in English.

17.6 This Agreement shall be governed by laws in force in India. Subject to the arbitration clause above, all disputes arising out of or in relation to this Agreement, shall be subject to the exclusive jurisdiction of the courts at **Mumbai** only.

17.7 In case of any change in applicable laws that has an effect on the terms of this Agreement, the Parties agree that the Agreement may be reviewed, and if deemed necessary by the Parties, make necessary amendments to the Agreement by mutual agreement in good faith, in case of disagreement obligations mentioned in this clause shall be observed.

18. POWERS TO VARY OR OMIT WORK

18.1 No alterations, amendments, omissions, additions, suspensions or variations of the work (hereinafter referred to as variation) under the Agreement shall be made by Service provider except as directed in writing by Bank. The Bank shall have full powers, subject to the provision herein after contained, from time to time during the execution of the Agreement, by notice in writing to instruct Service provider to make any variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If any suggested variations would, in the opinion of Service provider, if carried out, prevent them from fulfilling any of their obligations under the Agreement, they shall notify the Bank,

thereof, in writing with reasons for holding such opinion and Bank shall instruct Service provider to make such other modified variation without prejudice to the Agreement. Service provider shall carry out such variations and be bound by the same conditions, though the said variations occurred in the Agreement documents. If Bank confirms their instructions Service provider's obligations will be modified to such an extent as may be mutually agreed. If such variation involves extra cost, any agreed difference in cost occasioned by such variation shall be mutually agreed between the parties. In any case in which Service provider has received instructions from the Bank as to the requirement of carrying out the altered or additional substituted work, which either then or later on, will in the opinion of Service provider, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.

18.2 If any change in the work is likely to result in reduction in cost, the parties shall agree in writing so as to the extent of reduction in payment to be made to Service Provider, before Service provider proceeding with the change.

19. WAIVER OF RIGHTS

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this Agreement will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party. Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of any successive or other right, power or remedy on any other occasion.

20. LIMITATION OF LIABILITY

20.1 The maximum aggregate liability of Service Provider, subject to clause 20.3, in respect of any claims, losses, costs or damages arising out of or in connection with this Agreement shall not exceed the total Project Cost.

20.2 Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue.

20.3 The limitations set forth in Clause 20.1 shall not apply with respect to:

(i) claims that are the subject of indemnification pursuant to Clause 12[5] (infringement of third party Intellectual Property Right);

[5] Please see Clause 12 'IPR Indemnification'

(ii) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider;

(iii) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations;

(iv) Regulatory or statutory fines imposed by a government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider. For the purpose of clause 20.3(ii) "Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligation of the party under this Agreement and which causes injury, damage to life, personal safety, real property, harmful consequences to the other party, which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act for which such Party is legally liable. Notwithstanding the forgoing, Gross Negligence shall not include any action taken in good faith.

"Wilful Misconduct" means any act or failure to act with an intentional disregard of any provision of this Agreement, which a party knew or should have known if it was acting as a reasonable person, which would result in injury, damage to life, personal safety, real property, harmful consequences to the other party, but shall not include any error of judgment or mistake made in good faith.

21. FORCE MAJEURE

21.1 Notwithstanding anything else contained in the Agreement, neither Party shall be liable for any delay in performing its obligations herein if and to the extent that such delay is the result of an event of Force Majeure.

21.2 For the purposes of this clause, 'Force Majeure' means and includes wars, insurrections, revolution, civil disturbance, riots, terrorist acts, public strikes, hartal, bundh, fires, floods, epidemic, quarantine restrictions, freight embargoes, declared general strikes in relevant industries, Vis Major, acts of Government in their sovereign capacity, impeding reasonable performance of Service Provider and / or sub-contractor but does not include any foreseeable events, commercial considerations or those involving fault or negligence on the part of the party claiming Force Majeure.

21.3 If Force Majeure situation arises, the non-performing Party shall promptly notify to the other Party in writing of such conditions and the cause(s) thereof. Unless otherwise agreed in writing, the non-performing Party shall continue to perform its obligations under the

Agreement as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

21.4 If the Force Majeure situation continues beyond 30 (thirty) days, either Party shall have the right to terminate the Agreement by giving a notice to the other Party.Neither Party shall have any penal liability to the other in respect of the termination of this Agreement as a result of an event of Force Majeure. However, Service Provider shall be entitled to receive payments for all services actually rendered up to the date of the termination of this Agreement.

22. NOTICES

22.1 Any notice or any other communication required to be given under this Agreement shall be in writing and may be given by delivering the same by hand or sending the same by prepaid registered mail, postage prepaid, telegram or facsimile to the relevant address set forth below or such other address as each Party may notify in writing to the other Party from time to time. Any such notice given as aforesaid shall be deemed to be served or received at the time upon delivery (if delivered by hand) or upon actual receipt (if given by postage prepaid, telegram or facsimile).

22.2 A notice shall be effective when it is delivered or on the effective date of the notice, whichever is later.

22.3 The addresses for Communications to the Parties are as under.

(a) In the case of the Bank

State Bank of India, SB Global IT Centre
IT-RRBs & FO Tech Ops Department,
3rd Floor, Kapas Bhawan, Nirmala Devi Marg,
Sector 10, CBD Belapur, Navi Mumbai, Maharashtra– 400614

(b) In case of Service Provider

_____

_____

22.4 In case there is any change in the address of one Party, it shall be promptly communicated in writing to the other Party.

23. GENERAL TERMS & CONDITIONS

23.1 TRAINING: Service Provider shall train designated Bank officials on the configuration, operation/ functionalities, maintenance, support & administration for software, application architecture and components, installation, troubleshooting processes of the proposed Services as mentioned in this Agreement.

23.2 PUBLICITY: Service Provider may make a reference of the services rendered to the Bank covered under this Agreement on Service provider's Web Site or in their sales presentations, promotional materials, business plans or news releases etc., only after prior written approval from the Bank.

23.3 SUCCESSORS AND ASSIGNS: This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

23.4 NON-HIRE AND NON-SOLICITATION: During the term of this Agreement and for a period of one year thereafter, neither party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other party, or aid any third person to do so, without the specific written consent of the other party. However nothing in this clause shall affect the Bank's regular recruitments as per its recruitment policy and not targeted to the employees of Service provider.

23.5 SEVERABILITY: The invalidity or unenforceability of any provision of this Agreement shall not in any way effect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

23.6 MODIFICATION: This Agreement may not be modified or amended except in writing signed by duly authorized representatives of each party with express mention thereto of this Agreement.

23.7 ENTIRE AGREEMENT: The following documents along with all addenda issued thereto shall be deemed to form and be read and construed as integral part of this Agreement and in case of any contradiction between or among them the priority in which a document would prevail over another would be as laid down below beginning from the highest priority to the lowest priority:

(i) This Agreement;

(ii) Annexure of Agreement;

(iii) Purchase Order No._____ dated _____; and

(iv) RFP

23.8 PRIVITY: Neither this Agreement nor any provision hereof is intended to confer upon any person/s other than the Parties to this Agreement any rights or remedies hereunder.

23.9 DUE AUTHORISATION: Each of the undersigned hereby represents to the other that she/ he is authorized to enter into this Agreement and bind the respective parties to this Agreement.

23.10 COUNTERPART: This Agreement is executed in duplicate and each copy is treated as original for all legal purposes.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the date and day first mentioned above.

State Bank of India	**_____Service Provider**
By:	**By:**
Name:	**Name:**
Designation:	**Designation:**
Date:	**Date:**
WITNESS:	
1.	1.
2.	2.

ANNEXURE-A

DELIVERABLES/SCOPE OF WORK

The vendor has to ensure 99.95% uptime and optimum performance of the infrastructure mentioned in this RFP. It requires a dedicated team at SBI Sites possessing specialized skills and adequate experience. The team will be provided workstations / infrastructure for delivery of the services from Bank's offices at Navi Mumbai and Hyderabad. Access to the datacentres will be provided on need basis.

The brief details are mentioned as under:

i. Monitor/Manage/Maintain and manage Hardware and other platforms including OS, DB, and Application platforms, Middleware Application and Network, on a real-time basis for pro-active detection of issues, handling of internal user queries, providing MIS reports as required by the Bank and supporting the reconciliation issues. Identification of system defects proactively along with its resolution and to ensure a near defect free service.

ii. Ensure smooth functioning of every software and hardware components of the Infra in scope. 24x7x365 monitoring / administration of all the hardware equipment, OS, Application and Database. To provide maintenance support to the servers for the Bank's Critical Applications.

iii. Ensure consistency between Production and Disaster recovery setup, maintaining security across the platforms, Performance tuning of the entire setup, to identify bottlenecks on the system, upgrading of versions/patches and tracking all issues to closure.

iv. Conduct thorough review of the entire setup and see that the Procured infra is configured and utilized to the best of the available features and as per OEM recommended settings and industry best practices, in concurrence with the Bank. It would be a more insightful exercise requiring the review at both the hardware and software (Platform level) and ensure that the entire setup is optimized for best performance.

v. Vendor is required to have necessary support arrangement with the concerned OEMs in order to provide the necessary support on priority basis to meet the SLA requirements. The vendor will be provided necessary credentials for raising product specific tech support issues with OEMs.

vi. Vendor has to work in close coordination with respective application vendor teams with the ownership of activities under scope.

1. Description of Deliverables:

A. <u>Infrastructure Management service</u>

ITFO Infrastructure Management service is about ensuring 99.95% uptime of all listed applications hosted in the various data centres/Cloud for the department through

Administration and Support* for managing technology, information and data in a proactive way with the primary goal of minimum 99.95% uptime and keep the business as productive as possible.

The scope of these services starts from hardware/OS level to applications level (front/login pages) covering all attributes like networking, storage, data, security and cloud-based services and provide knowledgeable efficient human resources to keep everything working.

Installations, configurations, development, upgradation of firmware/versions/ patching, backup, all Security and Regulatory compliance, audits and DR-site management and maintaining various environment like Production, Pre-Prod, SIT, UATs/Development environments in primary/Secondary /Near sites for business continuity are major attributes included in the scope.

*Administration and support broadly covers Installation, Configuration, Maintenance, Performance Tuning, Monitoring, Backup, Troubleshooting and fixing issues of Hardware equipment / Operating Environments / Database / Application / Server/Underlying platform, including coordination with OEMs for fixing issues to ensure 99.95% System Uptime. The Services provided by the vendor will be on 24x7x365 basis. This also covers the scope of high-level automation by using scripts/ off-the-shelf-tools /in-house-developed-tools to replace repetitive manual activities with error-free robust systems/processes in place in most of the tasks performed. The Bank may procure tools and technology time to time from the market, the bidder shall use the same for carrying out day to day activities, as also automation of IT infrastructure monitoring and management.

Below table details the current scale of Infrastructure/Servers/Databases to be managed

Assets/Infrastructure	Total
Number of HP-UX Servers	965
Number of AIX Servers	285
Number of Linux Servers	430
Number of Windows Servers	200
Volume of Storage	3.5 PB
SAN Switches	95
Load Balancers	60
Physical Databases/Instances	1100

Middleware (WAS/'IHS'/MQ/IIB/SVN)	1800

B. Application Support service

Infra Application support service is meant to keep services of all the 'Applications' of IT-FO, up and running at all time with minimal downtime and provide necessary support in case of any change/ deployment at application level for Finacle suite and various other applications used for Foreign Offices in all operating environments (Production, Non-Prod , Development and Testing environments.)

IT Foreign Offices supports branches across the globe and run various applications. The exhaustive list of applications including Finacle suite of application is given below

i. Applications hosted at Data Centers

FEBA/YONO-GLOBAL Mobile App/YonoGlobal Web portal	Finacle Core	Finacle Treasury	FINACLE ALERT SERVICE
FinAssure	FNR	FI (Finacle Integrator)	FPH/FMH
Autosys	AMLOCK	E-Trade (FTI, FCC)	Connect 24 & CSIS
BEXI	Bridger	BCQP	Citrix thin client application
CRMNEXT	CCDP	Data Protector	ESB &/ Data power Gateway
GOLDEN-GATE	IBG Foreign Posting, IBG WEB SITE	MQ	MIS Online/Data Mart
OAO (Online Ac-count Opening)	OB (OPEN BANKING)	Omniflow (BPO for FOs)	Pelican
Redis	Swift Connect	SWIFT RECON	SVN
MFA Solution	Trade STP	CO Portal (Change Order portal)	ITFO-INFRA-POR-TAL
Whizible			

ii. List of Major Application Instances

Instance Type	Prod DC	Prod DR	Non-Prod	Total
Finacle CBS	52	56	252	360
CSIS/C24	56	56	140	252
Treasury	22	22	66	110
FEBA	30	30	30	90

Note: -

The assets and services mentioned in the scope are indicative. Actual Infrastructure and services may go up to 25% during the currency of the agreement and vendor has to support them.

2. Specifications, Performance Standards, and Functional Requirements:

The scope document is for the purpose of detailing the expected list of activities and areas of work.

(A) <u>INFRASTRUCTURE MANAGEMENT SERVICES</u>

Sr. No	Service Area	Requirements in brief
1.	**System Management**	i. User Account administration ii. Installation of current/future upgrades of hard-ware/software iii. Patch management and implementation with change order management (Refer Annexure-G). iv. Performance monitoring and fine-tuning v. Server Administration and Housekeeping vi. Change management and version control vii. Logs Review and analysis viii. Capacity management and planning ix. Hardware life cycle management. x. Documentation & maintenance of records/logs xi. Resolution of equipment issues with proper analysis and RCA. xii. Management of inventory of all assets xiii. Management and configuration of system resources /components (both physical and virtual) as and when required. xiv. Automation of various day-to-day jobs.

2.	**Storage Management**	i. Maintenance and creation of file systems ii. Space allocation to the respective server environment. iii. File server management and administration. iv. Capacity management and planning v. Installation, Administration, Configuration of various storage devices like SAN switches, media libraries etc. vi. Alert and resolve any performance issues and notify respective action owner. vii. Raising issues with the OEM vendor and arrange for resolution
3.	**Network Management**	i. Management of IP addresses allocation and configuration. ii. Coordination with the Network Team. iii. Management of SAN/NAS equipment. iv. Monitoring the network connection status on the devices. v. DNS, NTP ,SNMP, SMTP administration vi. Network/Patch Link termination vii. Network cabling in a structured way as and when required. viii. Migration from IPV4 to IPV6. ix. Maintenance of firewall access requests x. Management of network devices like load balancers, firewalls, N/W switches, routers etc.
4.	**Database Management**	i. Creation and management of database instances ii. Creation and allocation of file systems/flat files iii. encryption and data masking in all Databases

		iv.	Installing and configuration of DBMS (Oracle, mySQL, MS-SQL etc.)
		v.	Performing upgrades of the database and software to new release levels
		vi.	Starting up and shutting down the database services
		vii.	Managing the database's storage structures and schema objects, such as tables, indexes, and views
		viii.	Managing users and security of databases
5.	**Backup and recovery**	i.	All backups should be taken in a scheduled (Daily, Weekly, Monthly, and Yearly) manner as per the Bank's backup policy.
		ii.	Management of Scheduled and ad-hoc backups
		iii.	Monitoring of backups and restart of failed backups
		iv.	Restoration and recovery of backups as per Bank's Policy
		v.	Maintain proper backup schedules
		vi.	Facilitate onsite and off-site storage of tapes
		vii.	Maintain and submit periodic and ad hoc Backup re-ports.
6.	**Datacentre Operations**	i.	Physical Health Check and Infrastructure Monitoring
		ii.	Cabling and labelling of equipment
		iii.	Proper Rack Dressing
		iv.	Coordination with CDC team for various activities.
		v.	Installation/Movement of equipment within/to and from datacentres
		vi.	Management of all assets at various DCs/cloud.
7.	**DR Management**	i.	Handle DR operations and Participation in DR drills

		ii. Ensuring timely and proper DC - DR replication, and ensure that DR and standby applications are in sync iii. Configuration/Customization/development of scripts for automated replication iv. Ensuring consistency between DC, Failover and DR setups in co-ordination with application vendors. v. Managing Operation from DR in case of an associated incident/drills. vi. Managing RTO/RPO vii. Preparing reports for DR incidents/drills viii. Maintaining the same configuration between the sites.
8.	**Security and compliance**	i. Maintaining security posture and hardening of all devices ii. Configuration of servers /devices as per latest SCD policy prescribed by the Bank iii. Support during audits (IS audit, CSR, RFIA etc.) and other security review activities iv. Closure of VA-PT incidents and regulatory/internal/external audits & various other audit observations v. Maintaining confidentiality and integrity of all information as per bank's policy

(B) <u>APPLICATON SUPPORT SERVICES</u>

Sr. No.	Service Area	Requirements in brief
1.	**Support & services**	i. Support during infrastructure (Servers, Storage, switches etc.) patching activities i.e., bringing down all Environment services, bringing up the environment and related troubleshooting.

		ii. Production issues related to Finacle login and other functionalities/menu options. iii. Failover Support for Finacle Suite of Applications. iv. Support for CSIS, Connect24, FI interface, FDM, FIBEE, etc. in Production/non-Prod environment for Treasury, ESB, FEBA, E-Trade, LOS-LMS, CTS, and other third-party applications. v. Service configuration for Finacle suite of applications as and when required. vi. DB Restoration support, coordination and troubleshooting related issues whenever required for all application and all environments in-scope. vii. Application Infra related technical support during EOD for all environments, configuration and troubleshooting of related issues to ensure smooth EOD Operations. viii. Updating security certificates within the application whenever required. ix. Application patch deployment and sanity testing pertaining to application availability and functioning in Production/Non-Prod environments.
2.	**Interface Support**	i. Providing support for FI and Connect24 services in all environments (Prod/Non-Prod/Pre-Prod). ii. Debugging errors due to FI and Connect24. iii. Support for customizations of APIs. iv. Service request related to FI and Connect24. v. Real time monitoring and remediation of all the issues pertaining to interfaces faced by any interfacing application. vi. Configuration level changes required for monitoring services. vii. Ensuring that all the interfaces are properly secured and there is no possibility of sensitive information leakage.

3.	**Installation, Configuration & Administration**	i. Installation and configuration of Finacle and related services as per Bank's requests. ii. Post installation set up on C24 server (CBC/UNISER/CSIS/Refresh/Transmit service configuration etc.) iii. Configuring new CBC sections as per requirement (third party integration). iv. Setup and configuration of desired interfaces.
4.	**Audit observations compliance**	i. Closure of VA-PT/CSR/IS Review/Regulatory/internal/external & various other audit observations.
5.	**Service Integration**	i. Inputs and necessary configurations required for new integrations with Finacle suite of applications ii. New environment creation/ configuration/ administration for the in-scope applications. iii. Enhanced Support during Go Live of any new environment, interface, third-party integration, Annual closing, BCP exercise etc.
6.	**Network support and troubleshoot**	i. Identifying the issue and routing it to concerned team like network vendor/hardware vendor etc.
7.	**Support for monitoring service alerts**	i. Proactive Production/Pre-Prod/Non-Prod monitoring, real time support and responding to alerts generated by monitoring tool(s) provided by the Bank for all the in-scope applications by taking proactive remedial action with proper approval and laid down process. i. Changes in services related scripts at app level as per application monitoring service recommendations. ii. Coordinating with WAS and/or DB team to make changes at WAS level as per Application monitoring service recommendations. iii. Service requests related to Finacle login issues in desktops.
8.	**BCP Support**	i. DC-DR and multi node syncing.

		ii. DR/BCP switchover/switchback exercises etc. iii. Maintaining application sync between all Prod & Non- Prod environments. iv. Maintenance of application services for all in-scope applications in all environments during DR drills or as desired by the Bank with proper approvals.
9.	**Resource/Capacity Management**	i. Handling resource utilization issues in Production/Non-Production in real time. ii. Performance tuning and troubleshooting for Finacle suite of applications.

2.1 Service Provider undertakes and warrants to provide technical support with resolution time frame as per the matrix given below:

SERVICE MATRICES FOR RESPONSE AND RESOLUTION

Severity Level	**Description**	**Response Time**	**Resolution Time**
P1(Critical)	• Failure of a component where all of the following conditions are true; • critical business functions cannot be performed and • no workaround is available and • where a degraded mode of operation is not available or acceptable	Within 15 minutes	Up to 4 hours from reporting of the issue
P2(High)	Failure of a component where all of the following conditions are true; • a workaround or degraded performance is acceptable and • there is immediate financial or operations impact	<= 1 hour	Up to 8 hours from reporting of the issue

Severity Level	Description	Response Time	Resolution Time
	or • Failure of a component where: • a workaround or degraded performance is not acceptable and • there are no priority 1 conditions and • there is immediate financial or operations impact		
P3(Medium)	• Failure of a component where: • a workaround or degraded performance is acceptable • there is no immediate financial or operations impact	<= 4 hours	Up to 2 days from reporting of the issue
P4(Low)	• Configuration Activities • Closure of Audit/Security Observations • New environment creation etc. • Any other Requests as per the scope	<= 4 hours	Up to 4 days from reporting of the issue

3. Documentation: Few policies are mentioned below to which the bidder will have to adhere-

- ITFO Backup Policy
- Asset Management
- Capacity Management
- Logging, and Monitoring Management
- Patch Management
- Vendor Management
- User Management

4. Place of Service

1.	GITC Belapur, Navi Mumbai
2.	Rabale DC, Navi Mumbai
3.	Gachibowli, DC Hyderabad
4.	ITFO Department (Presently located at Kapas Bhavan, Sector-10 Belapur)

5. Standard Services

Standard services to be delivered under this Agreement are illustratively listed below:-

The brief services are mentioned below: 1. Infra Management services 2. Application Support Services More details for the above services and related responsibilities and availability are mentioned in Annexure-A (SOW)

6. Maintenance/ Upgrades

6.1 Service provider shall maintain and upgrade the software/ hardware during the contract period so that the software/ hardware shall, at all times during the contract period, meet the performance requirements as set forth in this Agreement. Service Provider shall, at no cost to the Bank, promptly correct any and all errors, deficiencies and defects in the software/ hardware.

6.2 Service Provider shall have the operational maintenance obligations (e.g., telephone support, problem resolution, on-site services) as mentioned in Annexure A.

7. Correction of Deficiencies in Deliverables

7.1 If Service provider is unable to correct all Deficiencies preventing acceptance of a deliverable or meet the performance requirements, for which Service provider is responsible within the timelines as mentioned in this Agreement, the Bank may at its discretion:

a) Impose penalty on Service Provider as mentioned under **Annexure E**.

b) Terminate this Agreement for cause in accordance with Clause 17 (except that the Bank is under no obligation to provide Service provider any further opportunity to cure) and recover its damages as set forth in this Agreement.

8. Risk Management

Service Provider shall identify and document the risk in delivering the Services. Service Provider shall identify the methodology to monitor and prevent the risk, and shall also document the steps taken to manage the impact of the risks.

ANNEXURE-B

INFRASTRUCTURE MANAGEMENT AND APPLICATION SUPPORT MATRICES

Urgency	Service level category	Service level object	Measurement range/criteria
Critical	Priority 1	Failure of a component where all of the following conditions are true; • critical business functions cannot be performed and • no workaround is available and • where a degraded mode of operation is not available or acceptable	Priority 1 Incidents include: • 100% of the users impacted Critical system outage or critical system usability limited (e.g., cannot logon, slow response time) with wide impact • Impacts financial close
High	Priority 2	Failure of a component where all of the following conditions are true; • a workaround or degraded performance is acceptable and • there is immediate financial or operations impact or • Failure of a component where: • a workaround or degraded performance is not acceptable and • there are no priority 1 conditions and • there is immediate financial or operations impact	Priority 2 Incidents could include: • 50% or more users affected. High priority financial issues which do not impact financial close, but may impact operations • High priority operations issues which do not directly impact the product, • The problem/issue prevents functioning of a critical component even though other components are working.

Urgency	Service level category	Service level object	Measurement range/criteria
Medium	Priority 3	Failure of a component where: • a workaround or degraded performance is acceptable • there is no immediate financial or operations impact	The problem / issue affects a minor function which does not impact operations of branches or any surrounding systems having impact on business operations.
Low	Priority 4	Configuration Activities • Closure of Audit/Security Observations • New environment creation etc. • Any other Requests as per the scope	

PRIORITY MATRIX FOR SERVICE AVAILABILITY

Highest priority 1 and lowest priority 4

Impact	Entire Site / Country		Critical Incidents Affecting a Set of Users / Application		Random users or single user	
Workaround/Solution Business Process	**Exists**	**Not Available**	**Exists**	**Not Available**	**Exists**	**Not Available**
Down	1	1	2	1	3	2
Not Immediately Affected	3	2	3	2	4	3
Not Affected	4	3	4	3	4	4

ANNEXURE-C

SERVICE LEVEL REPORTING/FREQUENCY

Activity	Frequency
Patch Deployment	Based on release of patch by OEM (Pre-production and Production)
Server availability	Availability of Application/Web and CBC servers for the whole month - Monthly
ADC's availability	Monthly - availability of ATM/POS/FEBA/SWIFT payments
Change Management	Weekly -Change management TAB defined
Monitoring Finacle Logs	Daily
Service desk ticketing review	Monthly
Health report	Daily
Incident report/RCA	Incident based
IR Dashboard	Monthly Review
Release Management	Monthly
Utilization report	Daily
CSIS support	Based on Planned DB activity
Monthly Review Presentation	Monthly (Includes DC and DR)
Housekeeping Activities	Every Week

SERVICE REVIEW MEETING

Service Review meeting shall be held annually/ half yearly. The following comprise of the Service Review Board:

- President: DGM (IT RRBs & FO–Tech Ops)
- Members: ITFO Infra Team

ANNEXURE-D

ESCALATION MATRIX

Service level Category	Response/Resolution Time	Escalation thresholds			
		Escalation Level 1		Escalation.....	
		Escalation to	Escalation Mode	Escalation to	Escalation Mode
Production Support		*<Name, designation contact no.>*		*<Name, designation contact no.>*	
Service Milestones		*<Name, designation contact no.>*		*<Name, designation contact no.>*	
Infrastructure Management		*<Name, designation contact no.>*		*<Name, designation contact no.>*	
Application Service Support		*<Name, designation contact no.>*		*<Name, designation contact no.>*	
Information Security		*<Name, designation contact no.>*		*<Name, designation contact no.>*	
Service Desk Support		*<Name, designation contact no.>*		*<Name, designation contact no.>*	

Escalation process:

1. All escalations will be sent by mail to Project Manager email ID who will be SPOC for this purpose. There will be a single email address which will be identified for Project Manager for this purpose.
2. Designated officers of respective Team will raise this escalation and each escalation will have unique number.
3. Category of Priority (P1,P2,P3 and P4) will be mentioned in the mail subject :
4. Count-down will be started from the mail timing for imposing penalty.
5. After resolution, PM will send response of the email which will be confirmed by the designated officers who raised the escalation.
6. Count-down will end on receiving response mail, subject to closure by the Bank and penalty will be calculated as per Annexure-E.

ANNEXURE-E

OTHER TERMS AND PENALTIES

PENALTY FOR NON-PERFORMANCE OF SLA

Sr. No.	Service Level Category	SLA Measure	Penalty Calculation
1	Application and Hardware Uptime	99.95% Average Application Uptime during support period to be calculated on monthly basis	0-15 Minutes - no penalty >15-30 Minutes Penalty @ Rs.5,000 per minute or part thereof >30-60 Minute Penalty @ Rs.10,000 per minute or part thereof >60 Minutes Penalty @ Rs.15,000 per minute or part thereof
2	Data Availability	Application data should be available/accessible at any instance of time	Rs.1,00,000 for every occasion of missing deadline of completing data ingestion within 3 hours of EOD excluding for the month-end.
3	Co-ordination with respective OEM for ticket resolution	1) Raising ticket (or workaround) in 15 minutes for High priority issue 2) Ticket resolution in 30 minutes for Medium priority issue 3) Ticket resolution in 45 minutes for Low priority issue	1) Rs.1,00,000 for every High priority issue missing resolution target 2) Rs.50,000 for every Medium priority issue missing resolution target 3) Rs.25,000 for every Low priority issue missing resolution target
4	RCA	Interim RCA in 2 days and final RCA observations to be shared within 5 days Both interim and final RCAs must be submitted to the Bank within the given timelines. RCA must be acceptable to the Bank.	Interim RCA: Rs.1,00,000 per incident for not providing interim RCA in 2 days. Final RCA: Rs.2,00,000 per incident for not providing final RCA in 5 days and additional Rs.50,000 per day and part thereof for further delays

5	Closure of VAPT	VAPT observations – All the points to be closed according to timelines given below; Critical – 20 days High – 30 days Medium – 45 days Low – 60 days	VAPT observations – Bank will inform the bidder on VAPT observation and timelines for calculating below penalties will start from the next day; Missing timeline of 20 days for Critical points – Rs.2,00,000 per instance per quarter Missing timeline of 30 days for High points – Rs.1,75,000 per instance per quarter Missing timeline of 45 days for Medium points – Rs.1,25,000 per instance per quarter Missing timeline of 60 days for Low points – Rs.1,00,000 per instance per quarter
6	Change Management	A work order will be given on mutually agreed timeline on any deliverable including development, enhancement, data sourcing, developing and modifications in monitoring dashboards, scheduling jobs, DAS data movement, etc.	Penalty of Rs.10,000 for delay of each one day or part thereof over committed timelines by vendor for any deliverable or change request
7	Non-availability of staff	Unavailability of any resource / role support in set up for agreed duration as per SLA	Rs.1,00,000 per person per week or part thereof for critical resources as mentioned in this Agreement

SEVERITY AND PENALTY MATRIX TABLE FOR "INFRASTRUCTURE MANAGEMENT SERVICES"

Severity	**Description**	**Response Time**		**Resolution time**		**Penalty**
		DC / DR	Near Site	DC / DR	Near Site	
Fatal Problem (P1) Work has come to halt	Disruption of the service (H/W, WEB, App, DB) for more than 15 minutes Or any of the application service not available attributable to the services in scope for more than 15 minutes	5 Mins	30 Mins.	2 Hours	4 Hours	0.5 of the payment for respective quarter for each 15 Mins of delay after

						initial 2 Hours
Severe Problem (P2)	Services though available but not working properly or working in a degraded mode	5 Mins.	1 Hours	3 Hours	4 Hours	0.5 of the payment for respective quarter for each 30 Mins of delay after initial 3 Hours
Important Problem (P3)	Non-transactional and only internal process are impacted	30 Mins	6 Hours	24 Hours	24 Hours	0.25 of the payment for respective quarter for each day of delay after 24 Hours
Minor Problem (P4)	Any delay in the scheduled/Planned activity like patch implementation / Fix pack implementation / SCD Implementation / parameterisation etc. for which the approval from bank has been obtained.	2 Hours	6 Hours	48 Hours	48 Hours	0.25 of the payment for respective quarter for each week of delay after 48 hours.

SEVERITY AND PENALTY MATRIX TABLE FOR "APPLICATION SERVICE SUPPORT"

The maximum value of penalty for quarter year would be restricted to the 10% of quarterly invoiced amount.

Severity level category	Severity Definition	Permissible Resolution Time (Without delay)	Penalty for delay (Beyond Permissible Resolution Time)
Fatal Problem (P1)	Failure of a component where all of the following conditions are true; • critical business functions cannot be performed and • no workaround is available and • where a degraded mode of operation is not available or acceptable	Up to 2 hours of reporting with 100% Compliance)	0.25% of the invoice amount for the quarter year for every 1 hours of delay after the maximum permissible resolution time per occurrence.
Severe Problem (P2)	Failure of a component where all of the following conditions are true; • a workaround or degraded performance is acceptable and • there is immediate financial or operations impact or • performance is not acceptable • and there are no priority 1 conditions and there is immediate financial or • operations impact	Up to 8 hours of reporting the issue with 100% Compliance)	0.25% of the invoice amount for the quarter year for every 1 hours of delay after the maximum permissible resolution time per occurrence.

Important Problem (P3)	Failure of a component where; • a workaround or degraded performance is acceptable and • there is immediate financial or operations impact	Up to 2 days of reporting the issue (90% Compliance)	0.25% of the invoice amount for the quarter year for every 1 days of delay after the maximum permissible resolution time per occurrence
Minor Problem (P4)	• Configuration Activities • Closure of Audit/Security Observations • New environment creation etc. • Any other Requests as per the scope.	Up to 4 days of reporting the issue (100% Compliance)	0.25% of the invoice amount for the quarter year for every 2 days of delay after the maximum permissible resolution time per occurrence

Additional Penalty Clause

- If the vendor fails to provide sufficient experienced staff as mentioned in the scope of work, Bank may impose a penalty @10% of the amount payable quarterly.
- There will be penalty of Rs.100 per day /per person on non-returning of access card to the bank on exit. This will be in addition to Rs.500 /- Penalty imposed by Bank's Security Department.
- If the vendor gives false compliance on closure of any security observation, there will be penalty of Rs.500 per observation per day till the time observation is closed.
- Stringent penalty will be imposed on any process violation. This penalty will be over and above the penalties mentioned in the SLA. The penalty may go up to 1% of the total project cost. Process document will be shared with the successful Vendor.
- All penalties mentioned in this RFP cover all such situations where the vendor fails to continue in the project. Fraction of month will be counted as full month. Total Project Cost will be calculated for the period project has run on pro rata basis.
- 1% of total Global revenue of the bidder will be imposed in case of breach of any GDPR regulation
- If any penalty is imposed by any Indian or foreign regulatory authority for leakage /theft of data due to negligence/ deliberate involvement of any vendor resource, full penalty will be borne by Vendor (Exclusive of the maximum penalty applicable).
- Vendor has to ensure deployment /presence of 90% of their onsite resources per day during the period

The above penalty shall be up to 10% of the project cost on pro rata basis on each occurrence. If the services are disrupted beyond the timeline provided in the above matrix, Bank may invoke the penalty clause and Bank shall have right to levy the aforesaid penalties.

Billing Process

- Remuneration of resource will be calculated on the basis of an individual's actual presence on the basis of evidence of attendance.
- Working for at least 8 hours in a day is mandatory.
- In case resource works for more than 8 hours to complete the task, no extra cost will be considered for payment, nor will this additional time be adjusted to complete 8 hours for any other working day.
- There will be total 24 working days in any month. i.e. a resource works on 24 days and 8 hours each day.
- At any cost, monthly bill of one resource will not go beyond the monthly cap of the resource. In case, resource attends more than 24 days in exigency, no extra cost will be calculated for the day.
- Resource can do work from home which should be pre-approved by Bank officials. In this case his VPN should be connected to the Bank for minimum eight hours.
- The discretion of allowing vendor for work from home (WFH) totally lies with the Bank and VPN should be used only in cases of extreme urgency.
- There will be only three status of Present/WHF/LEAVE for each resource. It should be shared with all stakeholders with contact details on daily basis. There will be no billing for the resource who is on leave.
- Vendor has to manage resources in surplus to meet minimum strength for each shift as per SLA.

ANNEXURE-F

Transition & Knowledge Transfer Plan

1. Introduction

1.1 This Annexure describes the duties and responsibilities of Service Provider and the Bank to ensure proper transition of services and to ensure complete knowledge transfer.

2. Objectives

2.1 The objectives of this annexure are to:

(1) ensure a smooth transition of Services from Service Provider to a New/Replacement SERVICE PROVIDER or back to the Bank at the termination or expiry of this Agreement;

(2) ensure that the responsibilities of both parties to this Agreement are clearly defined in the event of exit and transfer; and

(3) ensure that all relevant Assets are transferred.

3. General

3.1 Where the Bank intends to continue equivalent or substantially similar services to the Services provided by Service Provider after termination or expiry the Agreement, either by performing them itself or by means of a New/Replacement SERVICE PROVIDER, Service Provider shall ensure the smooth transition to the Replacement SERVICE PROVIDER and shall co-operate with the Bank or the Replacement SERVICE PROVIDER as required in order to fulfil the obligations under this annexure.

3.2 Service Provider shall co-operate fully with the Bank and any potential Replacement SERVICE PROVIDERs tendering for any Services, including the transfer of responsibility for the provision of the Services previously performed by Service Provider to be achieved with the minimum of disruption. In particular:

3.2.1 during any procurement process initiated by the Bank and in anticipation of the expiry or termination of the Agreement and irrespective of the identity of any potential or actual Replacement SERVICE PROVIDER, Service Provider shall comply with all reasonable requests by the Bank to provide information relating to the operation of the Services, including but not limited to, hardware and software used, inter-working, coordinating with other application owners, access to and provision of all performance reports, agreed procedures, and any other relevant information (including the configurations set up for the

Bank and procedures used by Service Provider for handling Data) reasonably necessary to achieve an effective transition, provided that:

3.2.1.1 Service Provider shall not be obliged to provide any information concerning the costs of delivery of the Services or any part thereof or disclose the financial records of Service Provider to any such party;

3.2.1.2 Service Provider shall not be obliged to disclose any such information for use by an actual or potential Replacement SERVICE PROVIDER unless such a party shall have entered into a confidentiality agreement; and

3.2.1.3 whilst supplying information as contemplated in this paragraph 3.2.1 Service Provider shall provide sufficient information to comply with the reasonable requests of the Bank to enable an effective tendering process to take place but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

3.3 In assisting the Bank and/or the Replacement SERVICE PROVIDER to transfer the Services the following commercial approach shall apply:

(1) where Service Provider does not have to utilize resources in addition to those normally used to deliver the Services prior to termination or expiry, Service Provider shall make no additional Charges. The Bank may reasonably request that support and materials already in place to provide the Services may be redeployed onto work required to effect the transition provided always that where the Bank agrees in advance that such redeployment will prevent Service Provider from meeting any Service Levels, achieving any other key dates or from providing any specific deliverables to the Bank, the Bank shall not be entitled to claim any penalty or liquidated damages for the same.

(2) where any support and materials necessary to undertake the transfer work or any costs incurred by Service Provider are additional to those in place as part of the proper provision of the Services the Bank shall pay Service Provider for staff time agreed in advance at the rates agreed between the parties and for materials and other costs at a reasonable price which shall be agreed with the Bank.

3.4 If so required by the Bank, on the provision of no less than 15 (fifteen) days' notice in writing, Service Provider shall continue to provide the Services or an agreed part of the Services for a period not exceeding **6 (Six)** months beyond the date of termination or expiry of the Agreement. In such event the Bank shall reimburse Service Provider for such elements of the Services as are provided beyond the date of termination or expiry date of the Agreement on the basis that:

(1) Services for which rates already specified in the Agreement shall be provided on such rates;

(2) materials and other costs, if any, will be charged at a reasonable price which shall be mutually agreed between the Parties.

3.5 Service Provider shall provide to the Bank an analysis of the Services to the extent reasonably necessary to enable the Bank to plan migration of such workload to a Replacement SERVICE PROVIDER provided always that this analysis involves providing performance data already delivered to the Bank as part of the performance monitoring regime.

3.6 Service Provider shall provide such information as the Bank reasonably considers to be necessary for the actual Replacement SERVICE PROVIDER, or any potential Replacement SERVICE PROVIDER during any procurement process, to define the tasks which would need to be undertaken in order to ensure the smooth transition of all or any part of the Services.

3.7 Service Provider shall make available such Key Personnel who have been involved in the provision of the Services as the Parties may agree to assist the Bank or a Replacement SERVICE PROVIDER (as appropriate) in the continued support of the Services beyond the expiry or termination of the Agreement, in which event the Bank shall pay for the services of such Key Personnel on a time and materials basis at the rates agreed between the parties.

3.8 Service Provider shall co-operate with the Bank during the handover to a Replacement SERVICE PROVIDER and such co-operation shall extend to, but shall not be limited to, inter-working, coordinating and access to and provision of all operational and performance documents, reports, summaries produced by Service Provider for the Bank, including the configurations set up for the Bank and any and all information to be provided by Service Provider to the Bank under any other term of this Agreement necessary to achieve an effective transition without disruption to routine operational requirements.

4. Replacement SERVICE PROVIDER

4.1 In the event that the Services are to be transferred to a Replacement SERVICE PROVIDER, the Bank will use reasonable endeavors to ensure that the Replacement SERVICE PROVIDER co-operates with Service Provider during the handover of the Services.

5. Subcontractors

5.1 Service Provider agrees to provide the Bank with details of the Subcontracts (if permitted by the Bank) used in the provision of the Services. Service Provider will not restrain or hinder its Subcontractors from entering into agreements with other prospective service

providers for the delivery of supplies or services to the Replacement SERVICE PROVIDER.

6. Transfer of Configuration Management Database

6.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the Configuration Management Database (or equivalent) used to store details of Configurable Items and Configuration Management data for all products used to support delivery of the Services.

7. Transfer of Assets

7.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of the Agreement Service Provider shall deliver to the Bank the Asset Register comprising:

(1) a list of all Assets eligible for transfer to the Bank; and

(2) a list identifying all other Assets, (including human resources, skillset requirement and know-how), that are ineligible for transfer but which are essential to the delivery of the Services. The purpose of each component and the reason for ineligibility for transfer shall be included in the list.

7.2 Within 1 (one) month of receiving the Asset Register as described above, the Bank shall notify Service Provider of the Assets it requires to be transferred, (the "Required Assets"), and the Bank and Service Provider shall provide for the approval of the Bank a draft plan for the Asset transfer.

7.3 In the event that the Required Assets are not located on Bank premises:

(1) Service Provider shall be responsible for the dismantling and packing of the Required Assets and to ensure their availability for collection by the Bank or its authorized representative by the date agreed for this;

(2) any charges levied by Service Provider for the Required Assets not owned by the Bank shall be fair and reasonable in relation to the condition of the Assets and the then fair market value; and

(3) for the avoidance of doubt, the Bank will not be responsible for the Assets.

7.4 Service Provider warrants that the Required Assets and any components thereof transferred to the Bank or Replacement SERVICE PROVIDER benefit from any remaining manufacturer's warranty relating to the Required Assets at that time, always provided such warranties are transferable to a third party.

8. Transfer of Software Licenses

8.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank all licenses for Software used in the provision of Services which were purchased by the Bank.

8.2 On notice of termination of this Agreement Service Provider shall, within 2 (two) week of such notice, deliver to the Bank details of all licenses for SERVICE PROVIDER Software and SERVICE PROVIDER Third Party Software used in the provision of the Services, including the terms of the software license agreements. For the avoidance of doubt, the Bank shall be responsible for any costs incurred in the transfer of licenses from Service Provider to the Bank or to a Replacement SERVICE PROVIDER provided such costs shall be agreed in advance. Where transfer is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

8.3 Within 1 (one) month of receiving the software license information as described above, the Bank shall notify Service Provider of the licenses it wishes to be transferred, and Service Provider shall provide for the approval of the Bank a draft plan for license transfer, covering novation of agreements with relevant software providers, as required. Where novation is not possible or not economically viable the Parties will discuss alternative licensing arrangements.

9. Transfer of Software

9.1 Wherein State Bank of India is the owner of the software, 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver, or otherwise certify in writing that it has delivered, to the Bank a full, accurate and up to date version of the Software including up to date versions and latest releases of, but not limited to:

(a) Source Code (with source tree) and associated documentation;

(b) application architecture documentation and diagrams;

(c) release documentation for functional, technical and interface specifications;

(d) a plan with allocated resources to handover code and design to new development and test teams (this should include architectural design and code 'walk-through');

(e) Source Code and supporting documentation for testing framework tool and performance tool;

(f) test director database;

(g) test results for the latest full runs of the testing framework tool and performance tool on each environment; and

10. Transfer of Documentation

10.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up-to date set of Documentation that relates to any element of the Services as defined in Annexure A.

11. Transfer of Service Management Process

11.1 6 (six) months prior to expiry or within 2 (two) weeks of notice of termination of this Agreement Service Provider shall deliver to the Bank:

(a) a plan for the handover and continuous delivery of the Service Desk function and allocate the required resources;

(b) full and up to date, both historical and outstanding Service Desk ticket data including, but not limited to:

(1) Incidents;

(2) Problems;

(3) Service Requests;

(4) Changes;

(5) Service Level reporting data;

(c) a list and topology of all tools and products associated with the provision of the Software and the Services;

(d) full content of software builds and server configuration details for software deployment and management; and

(e) monitoring software tools and configuration.

12. Transfer of Knowledge Base

12.1 6 (six) months prior to expiry or within 2 (two) week of notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date cut of content from the knowledge base (or equivalent) used to troubleshoot issues arising with the Services but shall not be required to provide information or material which Service Provider may not disclose as a matter of law.

13. Transfer of Service Structure

13.1 6 (six) months prior to expiry or within 2 (two) weeks' notice of termination of this Agreement Service Provider shall deliver to the Bank a full, accurate and up to date version of the following, as a minimum:

(a) archive of records including:

(1) Questionnaire Packs;

(2) project plans and sign off;

(3) Acceptance Criteria; and

(4) Post Implementation Reviews.

(b) Program plan of all work in progress currently accepted and those in progress;

(c) latest version of documentation set;

(d) Source Code (if appropriate) and all documentation to support the services build tool with any documentation for 'workarounds' that have taken place;

(e) Source Code, application architecture documentation/diagram and other documentation;

(f) Source Code, application architecture documentation/diagram and other documentation for Helpdesk; and

(g) project plan and resource required to hand Service Structure capability over to the new team.

14. Transfer of Data

14.1 In the event of expiry or termination of this Agreement Service Provider shall cease to use the Bank's Data and, at the request of the Bank, shall destroy all such copies of the Bank's Data then in its possession to the extent specified by the Bank.

14.2 Except where, pursuant to paragraph 14.1 above, the Bank has instructed Service Provider to destroy such Bank's Data as is held and controlled by Service Provider, 1 (one) months prior to expiry or within 1 (one) month of termination of this Agreement, Service Provider shall deliver to the Bank:

(1) An inventory of the Bank's Data held and controlled by Service Provider, plus any other data required to support the Services; and/or

(2) a draft plan for the transfer of the Bank's Data held and controlled by Service Provider and any other available data to be transferred.

15. Training Services on Transfer

15.1 Service Provider shall comply with the Bank's reasonable request to assist in the identification and specification of any training requirements following expiry or termination. The purpose of such training shall be to enable the Bank or a Replacement SERVICE PROVIDER to adopt, integrate and utilize the Data and Assets transferred and to deliver an equivalent service to that previously provided by Service Provider.

15.2 The provision of any training services and/or deliverables and the charges for such services and/or deliverables shall be agreed between the parties.

15.3 Subject to paragraph 15.2 above, Service Provider shall produce for the Bank's consideration and approval 6 (six) months prior to expiry or within 10 (ten) working days of issue of notice of termination:

(1) A training strategy, which details the required courses and their objectives;

(2) Training materials (including assessment criteria); and

(3) a training plan of the required training events.

15.4 Subject to paragraph 15.2 above, Service Provider shall schedule all necessary resources to fulfil the training plan, and deliver the training as agreed with the Bank.

15.5 SERVICE PROVIDER shall provide training courses on operation of licensed /open source software product at Bank's Premises, at such times, during business hours as Bank may reasonably request. Each training course will last for 6 hours. Bank may enroll up to 10 % of its staff or vendor employees of the new/replacement service provider in any training course, and Service Provider shall provide a hard copy of the Product (licensed or open sourced) standard training manual for each enrollee. Each training course will be taught by a technical expert with no fewer than 5 years of experience in operating related software system. SERVICE PROVIDER shall provide the training without any additional charges.

16. Transfer Support Activities

16.1 6 (six) months prior to expiry or within 10 (ten) Working Days of issue of notice of termination, Service Provider shall assist the Bank or Replacement SERVICE PROVIDER to develop a viable exit transition plan which shall contain details of the tasks and responsibilities required to enable the transition from the Services provided under this Agreement to the Replacement SERVICE PROVIDER or the Bank, as the case may be.

16.2 The exit transition plan shall be in a format to be agreed with the Bank and shall include, but not be limited to:

(1) a timetable of events;

(2) resources;

(3) assumptions;

(4) activities;

(5) responsibilities; and

(6) risks.

16.3 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER specific materials including but not limited to:

(a) Change Request log;

(b) entire back-up history; and

(c) dump of database contents including the Asset Register, problem management system and operating procedures. For the avoidance of doubt this shall not include

proprietary software tools of Service Provider which are used for project management purposes generally within Service Provider's business.

16.4 Service Provider shall supply to the Bank or a Replacement SERVICE PROVIDER proposals for the retention of Key Personnel for the duration of the transition period.

16.5 On the date of expiry Service Provider shall provide to the Bank refreshed versions of the materials required under paragraph 16.3 above which shall reflect the position as at the date of expiry.

16.6 Service Provider shall provide to the Bank or to any Replacement SERVICE PROVIDER within 14 (fourteen) Working Days of expiry or termination a full and complete copy of the Incident log book and all associated documentation recorded by Service Provider till the date of expiry or termination.

16.7 Service Provider shall provide for the approval of the Bank a draft plan to transfer or complete work-in-progress at the date of expiry or termination.

17. Use of Bank Premises

17.1 Prior to expiry or on notice of termination of this Agreement, Service Provider shall provide for the approval of the Bank a draft plan specifying the necessary steps to be taken by both Service Provider and the Bank to ensure that the Bank’s Premises are vacated by Service Provider.

17.2 Unless otherwise agreed, Service Provider shall be responsible for all costs associated with Service Provider’s vacation of the Bank’s Premises, removal of equipment and furnishings, redeployment of SERVICE PROVIDER Personnel, termination of arrangements with Subcontractors and service contractors and restoration of the Bank Premises to their original condition (subject to a reasonable allowance for wear and tear).

ANNEXURE-G

CHANGE MANAGEMENT PROCESS

All changes will be categorized in accordance with ITIL / ITSM standards into one of: Routine Changes, Normal Changes, Emergency Changes and Project Changes, which are defined below.

For the avoidance of doubt, "Routine Changes", "Normal Changes" and "Emergency Changes" all refer to operational changes to SBI service and do not need to go through the formal Change Control Procedure, except where there is a cost implication. Project Changes, including any changes to the scope and/or price of the Services provided by vendor will need to go through the formal Change Control procedure.

Routine, Normal and Emergency Changes can be requested by SBI or vendor staff, but will be approved by authorized SBI personnel prior to implementation unless pre-approved (i.e. a Routine Change) or required to resolve a critical incident (i.e. an Emergency Change).

To provide on-time delivery of changes into the SBI environment and minimize service interruption, we employ a Change Management process. Change Management controls and manages request to change the solution as proposed for application services. The process maintains proper balance between the need for change and potential detrimental impact of the change while maintaining the integrity of the infrastructure in a structured, cost-effective manner to meet business requirements.

Change Management methodically assesses the impact of proposed changes to the service environment to mitigate potential risks and to realize projected business benefits in a timely fashion.

This process controls and manages change to the IT infrastructure by authorizing and reviewing the test, implementation, and release plans. It uses standard tools and documented procedures for accepting, approving, coordinating, and escalating changes.

Change Management consists of the following key activities:

Change Acceptance - Filters and documents request for changes (RFCs), verifying completeness of information and requestor authorization and establishing priority based on business impact; requests are acknowledged and classified as standard, non-standard, or urgent.

- **Urgent requests** are expedited through the Change Advisory Board/Emergency Committee (CAB/EC) and implemented as quickly as possible to prevent or mitigate negative business impact.
- **Standard requests** that are pre-approved or relatively common, follow predefined templates.
- **Non-standard requests** are assessed for technical and business impact (major, significant, or minor).

RFC Approval – Selects the appropriate approvers based on change classification (standard, non-standard, or urgent) and change impact (major, significant, or minor)

Change Coordination - Uses the CAB/EC to review and approve release and test plans for risk and impact, appropriate detail, back out plans, and cost justification.

Once the release is built and tested, the CAB/EC reviews the build and test results before approving the implementation. A post-implementation review confirms each change meets business and functional objectives.

Any request for a change must be documented in the Change Request form and will be evaluated technically and commercially. The cost implications may be monetary and/or in terms of time, and

are an outcome of how much effort will be required to implement the change. Input from vendor consultants will be required to determine these costs. Any change must be approved through the Change Control procedure.

The changes will be dealt in accordance with below mentioned table.

Change Type	Minimum Lead Time (calendar days)	Definition
Major	15	Is a change that has high risk and high impact on customer or vendor business and can potentially cause a critical Incident (Priority 1) on Key Production Environment (KPE). Fifteen (15) calendar days prior to implementation start date.
Normal	7	Any temporary or permanent change to a service or the infrastructure with a certain level of risk within a managed environment. Seven (7) calendar days prior to implementation start date.
Urgent Normal	3	Changes which are considered as urgent by the business. They will follow the Normal Change process flow, but by the nature of their potential impact to the business, they by-pass normal lead times. Three (3) calendar days prior to implementation start date.
Standard (Routine)	1*	Standard Changes with Low Impact and Risk. These changes are pre-approved. Once approved as a routine (pre-approved) change – One (1) *Business day prior to implementation start date.
Emergency	0	These are the changes which are a result of sudden loss or reduction of service to the managed environment. Emergency Changes are always derived from business-critical Incidents (Priority 1 or 2 only) or an imminent outage that will have a critical impact to the business. No lead time for Emergency changes, they must follow the Emergency Change process.

ROUTINE CHANGES

Routine Changes are intended to cover specific changes that will have a requirement to be executed many times following a consistent process or set of instructions. Routine changes will be defined on a need basis and will result in the creation of a unique process and instruction for the execution of each change. Each routine change must be approved and signed off by both SBI and Vendor before it is deployed into a Routine Change library, after which time the execution of the change may be requested and executed, on the assumption that each is pre-authorized by the initial sign off. No authorization is required to execute a Routine Change once the initial process is signed off. Routine Change implementation will commence within the agreed time scale (see below) unless an alternate timeline of time dependency is identified in the Routine Change instructions.

Any Routine Change beyond the Scope of Work defined in this document will be charged at a mutually agreed rate.

Routine Change Responsibilities

Activity	vendor	SBI
Receipt of requests from SBI to define Routine Changes.	✓	
The recommendation to specify a regularly repeated Normal Changes as a Routine Change to improve control, efficiency or speed of execution.	✓	
The production of Routine Change process documents and Instructions.	✓	
The presentation of proposed Routine Change documentation to SBI for approval.	✓	
Commence execution of an approved routine change within the agreed timeframe.	✓	
Maintain a library of approved routine changes and their associated documentation.	✓	
Provide a unique identifier to SBI to be used when requesting execution.	✓	
Identification of the setup costs and execution costs for each routine change to SBI.	✓	
Requesting routine change creation.		✓

Activity	vendor	SBI
Approval of newly created Routine Change processes and instructions.		✓
Ensuring all Routine Change execution requests are routed via vendor.		✓
Ensure all Routine Change request executions use the unique identifier for each (as supplied by vendor).		✓
Identifying any changes within the SBI environment not under vendor control that invalidate or require amendments to be made to the Routine Change library.		✓
Approval or rejection of setup and execution costs for routine changes.		✓

NORMAL CHANGES

Normal Changes are those that are not a Routine Change or Project Change and require suite able planning and approval to ensure that unplanned impact or failure is minimized. Normal changes must be formally requested via the creation of a Request for Change form (RFC). Vendor may request Normal Changes or SBI authorized staff. Normal changes will be authorized solely via the vendor and SBI nominated members.

Any Normal Change beyond the current scope of work will have to be jointly assessed, and if approved, will have to be operationalized at a mutually agreed rate.

Normal Change Responsibilities

Activity	vendor	SBI
Logging of Normal Change Requests.	✓	
Evaluation of change impact and risk.	✓	
Production of technical implementation and back out plans for changes.	✓	
Attendance and management of weekly CAB meetings / teleconference.	✓	
Approval of changes at CAB meetings.	✓	
Rejection of changes where risk / planning is insufficient.	✓	

Activity	vendor	SBI
Identification of costs to SBI where changes fall outside of the scope of the vendor service.	✓	
Provision of forms / media for SBI to request Normal Changes.	✓	
Request Normal Changes using supplied forms / media.		✓
Identification of business need, impact and risk on changes for components and services affected by the change that fall outside of the scope of the vendor service.		✓
Attendance of appropriate authorized personnel at CAB meetings / teleconference.		✓
Approval of changes.		✓
Rejection of changes.		✓

EMERGENCY CHANGES

Emergency Changes will only derive from a service failure (incident) or an imminent service failure (e.g. security breach / vulnerability). These are normal changes that due to the criticality to apply, will require the approval stage of the change management process to be completed retrospectively. This is an exceptional situation and will normally not be the preferred way of processing an individual change.

Typically, an emergency change is one that is required where it is better to do something, regardless of the risk of lack of preparation, than to do nothing. Emergency changes may also be requested to bypass the normal change process if SBI states at the relevant time, it is willing to mitigate vendor against any resultant damage / failure and the effort required to correct or back out the change.

PROJECT CHANGES

Any changes that are of a size to require project management will be handled on a formal Change Control Procedure basis. Typically, any change that requires in excess of 5-man days effort to deploy or involves any other change to the scope of vendor's services and charges is considered to be a Project Change.

Dependencies

1. SBI will provide the vendor onsite staff seat, PC and Phone for providing onsite support from client premises.
2. In case if a resource resigns, time for replacement of vendor headcount talent would be 3 months from the date of notice and for replacement of partner resource, 45 days from date of notice by client.
3. No provision for any kind of support for any third-party applications deployed in the landscape.
4. SBI will provide relevant access to vendor personnel as needed to carry out activities contributing to work.
5. Day-to-day consumables & backup media are provided by the Bank.
6. Any change in the baseline will be handled by Change Control mechanism.
7. All project related activities or build / transform will be treated as project, and need to go through change management route.
8. Bank is responsible for purchasing additional infrastructure to meet the capacity demands and growth of the applications.
9. SBI has valid product support contract with respective OEMs for Finacle suite of applications.
10. Vendor will coordinate and participate in DR drills along with application vendors by leveraging auto DR failover & data replication tools provided by the Bank to meet the RTO and RPO.
11. Vendor standard service levels will exclude incidents that relate to facilities, hardware and software maintenance agreements.
12. Support for any hardware or software that is end of service or no longer has vendor support will be on best effort & financial viable basis only and will not be subject to SLA's.
13. Service outages due to DC external facilities such as AC \ Power \ Cooling \ Cabling will be excluded from SLA calculation.
14. Any server downtime due to security issue or virus outbreak will be out of scope.
15. Any server downtime issue due to hardware failure, as H/w support and warranty is out of scope.
16. IT Security policies, procedures and guidelines are owned and maintained by Bank. Bank to provide the copy of existing security policies and controls to vendor during transition stage.
17. SBI existing security policies and infrastructure are complying to PCI DSS, RBI Guidelines, Country specific, Privacy regulations & ISO 27001 standards. Also, SBI have deployed the required security tools in compliance with security policies, regulatory requirements, data privacy etc. and will remain responsible for compliance to any such requirement that may arise.
18. Vendor services are limited to complying with Bank Security guidelines for vendor Services for all Applications in-scope; Complying to any other regulatory compliance and country specific regulations are not part of scope.
19. It is assumed that Vulnerability Assessment & Penetration Testing will be performed by SBI or their designated third party. Vendor team will perform remediation activities based on identified vulnerability reports & recommendations provided for Infrastructure being managed by vendor. Any post remediation scans will be Bank/ 3rd party responsibility.
20. Any application upgrade evaluations, recommendations and implementations will be out of scope and requires following change management process.

21. Any other security controls needed from vendor will be discussed & vendor will submit a Change request for inclusion of the same in scope.
22. In case of any compliance changes leading to requirement of vendor security efforts for deploying additional controls on vendor Managed Servers, which would be handled through change requests in mutual discussion with Bank.
23. All communications, documentation will be in English language only.

XXXX