भारतीय लघु उद्योग विकास बैंक

Small Industries Development Bank of India

डाटा सेंटर व डीआर साइट में इंफ्रास्ट्रक्चर सेवाओं के प्रबंधन हेतु प्रस्ताव का आमंत्रण

REQUEST FOR PROPOSAL

[REVISED RFP ISSUED ON APRIL 01, 2021 ALONG WITH PRE-BID CLARIFICATIONS]

DATACENTER & DR SITE INFRASTRUCTURE MANAGED SERVICES

(November 01, 2021 till October 31, 2026)

टेंडर सं. / Tender No.	400/2021/1619/BYO/ITV
टेंडर जारी करने की तिथि / Tender Issue Date	March 16, 2021
बोली जमा करनी की अंतिम तिथि / Last date for bid submission	April 15, 2021
बयाना जमा राशि / Earnest Money Deposit (Refundable without Interest)	रु. 40,50,000/- (रु Forty Lakh Fifty Thousand only)
टेंडर मूल्य /Tender Cost (Non Refundable)	रु.11,800/- (₹ Eleven Thousand Eight Hundred only), inclusive of GST

भारतीय लघु उद्योग विकास बैंक
स्वावलंबन भवन, सी-11, जी ब्लाक,
बांद्रा कुर्ला काम्प्लेक्स, बांद्रा (पू.), **मुम्बई – 400051**

SMALL INDUSTRIES DEVELOPMENT BANK OF INDIA
Swavlamban Bhavan, C-11, ‘G’ Block,
Bandra Kurla Complex, Bandra (E), **Mumbai - 400 051**

Table of Contents

Appendix Details

Appendix	Description
Appendix-I	List of SIDBI offices
Appendix-II	List of Hardware at Datacentre, Mumbai
Appendix-III	List of Hardware at Disaster Recovery (DR) Site, Chennai
Appendix-IV	List of Servers at other Offices
Appendix-V	Office Wise list of Network Equipment
Appendix-VI	List of Hardware at Mumbai Office
Appendix-VII	Details of Applications & Hosting Platform (Middleware Software Tools)
Appendix-VIII	Details of Hardware for AMC Services
Appendix-IX	Details of Security Devices

***** All the appendices are given in SIDBI.Outsourcing.RfP.Appendix.zip***

Annexure Details

Annexure(s)	
1.	Annexure I – Eligibility Bid - Forwarding Letter
2.	Annexure II – General Information about Bidder
3.	Annexure III – Response to the Minimum Eligibility Criteria
4.	Annexure IV – Clean Track Record & Other Declarations
5.	Annexure V – Conformity of Hardcopies
6.	Annexure VI – Statement of Deviations
7.	Annexure VII – Letter of Competence
8.	Annexure VIII – Power of Attorney
9.	Annexure IX – Letter of Conformity
10.	Annexure X – Resource Deployment Plan
11.	Annexure XI – Commercial Bid – Forwarding Letter
12.	Annexure XII – Non-Disclosure Agreement
13.	Annexure XIII – Bank Mandate Form
14.	Annexure XIV – EMD / Bid Security Form
15.	Annexure XV – Performance Bank Guarantee
16.	Annexure XVI – Pre-Contract Integrity Pact
17.	Annexure XVII – Commercial Bid Format

***** All the annexures are given in SIDBI_DC_DR_INFRA_Annexure.zip***

1. Critical Information/ महत्वपूर्ण सूचना

1.1 Details of Critical Information

SNo. क्र.सं.	Events / कार्यक्रम	Date/ तिथि	Time/ समय
1	Last date for seeking clarifications for pre-bid meeting/ पूर्व-बोली बैठक के लिए स्पष्टीकरण की मांग की अंतिम तिथि	March 25, 2021 / 25 मार्च, 2021	6:00pm
2	Pre-bid meeting (*no clarifications would be given after pre-bid meeting*)/ पूर्व-बोली बैठक के बाद कोई भी स्पष्टीकरण नहीं दिया जाएगा।	March 26, 2021 / 26 मार्च, 2021	12:00pm
3	Last date for submission of bids/ बोली जमा करने की अंतिम तिथि	April 15, 2021 / 15 अप्रैल, 2021	3:30pm
4	बोली जमा और पूर्व-बोली बैठक करने का पता/ Address for Bid Submission and Pre-bid meeting		
	महाप्रबन्धक (आई.टी.वी.) भारतीय लघु उद्योग विकास बैंक, तीसरा तल, इन्फॉर्मेशन टेक्नालजी वर्टिकल, स्वावलम्बन भवन, प्लाट सी-11, जी ब्लाक, बांद्रा कुर्ला काम्प्लेक्स, बांद्रा(पू.), **मुम्बई – 400 051,** दूरभाष: 022-67531100 / 67531251 , फैक्स: 022-67531236	**General Manager (ITV)** Small Industries Development Bank of India, 3rd Floor, Information Technology Vertical, Swavlamban Bhawan, Plot No. C-11, G Block, Bandra Kurla Complex, Bandra (E), **Mumbai - 400 051** Phone: 022-67531100/ 67531251 Fax: 022-67531236	
5	Date & Time of Opening of Minimum Eligibility bid & Technical bid/ न्यूनतम व तकनीकी बोली खोलने की तिथि व समय	April 15, 2021 / 15 अप्रैल, 2021	4:00pm
6	Date and time of opening of commercial bids / वाणिज्यिक बोली खोलने की तिथि व समय	To be intimated at a later date / बाद में सूचित किया जायेगा	
7	Bid Validity/ बोली के वैद्यता	**Six Months** from the last date of bid submission/ बोली जमा करने की अंतिम तिथि से छह महीने तक।	
8	Presentations to be made by bidders/ बोलीदाताओं द्वारा की जाने वाली प्रस्तुतियाँ	The bidders are required to arrange for presentation. Date would be intimated after bid submission / बोलीदाताओं को प्रस्तुतियों का प्रबंध करना होगा।	
9	Contact details of SIDBI officials/ सिडबी अधिकारियों के संपर्क विवरण	**Narender Kumar, AGM (Systems)** 022-67531238, narender@sidbi.in **Rajesh Joshi, AGM (Systems)** 022-67531251, rjoshi@sidbi.in **P K Vijayvargia, GM (ITV)** (0522) 4261657, pkvijay@sidbi.in	

SNo. क्र.सं.	Events / कार्यक्रम	Date/ तिथि	Time/ समय
10	Earnest Money Deposit/ बयाना जमा राशि	**रु. 40,50,000/-** (₹ Forty Lakh Fifty Thousand only)	
11	Tender Cost/ टेंडर मूल्य	रु.11,800/- (₹ Eleven Thousand Eight Hundred only), incl. of GST	
12	Independent External Monitor/ स्वतंत्र बाह्य मॉनिटर		
	श्री नागेश्वर राव कोरीपल्ली. आईआरएस (सेवानिवृत्त) 38, ट्रेल्स, मानिकोंडा, आर आर जिला, **हैदराबाद – 500089** मोबाइल : 9788919555 ईमेल : knageshwarrao@gmail.com	Shri Nageshwar Rao Koripalli, IRS(Retd.) 38, The Trails, Manikonda, R. R. District **Hyderabad – 500089** Mobile: 9788919555 Email : knageshwarrao@gmail.com	

1.2 Important Note

1.2.1 SIDBI reserves the right to change dates without assigning any reasons thereof. Intimation of the same shall be notified on the Bank's website.

1.2.2 If a holiday is declared on the dates mentioned above, the tender shall be received / opened on the next working day at the same time specified above and at the same venue unless communicated otherwise.

****

2. Abbreviations

Abbreviation	Full Form
ATS	Annual Technical Support
AMC	Annual Maintenance Contract
BO	Branch Office of the Bank.
BG	Bank Guarantee
CMDB	Configuration Management Database
DBA	Data Base Administrator
DC	Datacentre of the Bank
DR or DRS	Disaster Recovery Site of the Bank
EMD	Earnest Money Deposit
EMS	Event Monitoring Service
FM	Facility Management
FMS	Facility Management Services
GST	Goods and Service Tax
HO	Head Office of the Bank.
IIMC	IT Infrastructure Management Centre
IMO	Infrastructure Management Outsourcing
IPv6	Internet Protocol Version 6
IPv4	Internet Protocol Version 4
ITIL	IT Information Library
LAN	Local Area Network
MAF	Manufacturer Authorisation Form
MCV	Monthly Contract Value
NEFT	National Electronic Fund Transfer
OEM	Original Equipment Manufacturer
PBG	Performance Bank Guarantee
PoC	Proof of Concept
RfP	Request for Proposal
RO	Regional Office of the Bank
SDWAN	Software Defined Wide Area Network
TCO	Total Cost of Ownership
LD	Liquidated Damages
FM	Facility Management
TCV	Total Contract Value (which is equal to TCO)
WAN	Wide Area Network

****

3. Introduction and Disclaimers

3.1 Preface

3.1.1 This Request for Proposal document ('RFP document' or RFP or RfP) has been prepared solely for the purpose of enabling SIDBI to select a Service Provider for "Outsourcing of Infrastructure Managed Services" for Datacentre & Disaster Recovery site (DC & DR) and Application Support Management Services, for a period of 05 years from November 01, 2021 to October 31, 2026.

3.1.2 The RfP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between SIDBI and the successful Bidder as identified by SIDBI, after completion of the selection process as detailed in this document.

3.2 Information Provided

3.2.1 The RfP document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with SIDBI.

3.2.2 Neither SIDBI nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document.

3.2.3 Neither SIDBI nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.

3.3 For Respondent only

3.3.1 The RFP document is intended solely for the information of the party to whom it is issued ("the Recipient" or "the Respondent" or "the Bidder")

3.4 Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, Bank and its directors, officers, employees, contractors, representatives, agents, and advisers disclaim all liability from any loss, claim, expense (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursements incurred therein or incidental thereto) or damage, (whether foreseeable or not) ("Losses") suffered by any person acting on or refraining from acting because of any presumptions or information (whether oral or written and whether express or implied), including forecasts, statements, estimates, or projections contained in this RFP document or conduct ancillary to it whether or not the Losses arise in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of Bank or any of its directors, officers, employees, contractors, representatives, agents, or advisers.

3.5 Costs to be borne by Respondents

All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to the attendance at meetings, discussions, demonstrations, presentations, site visits etc. and providing any additional information required by SIDBI, will be borne entirely and exclusively by the Respondent.

3.6 No Legal Relationship

No binding legal relationship will exist between any of the Respondents and SIDBI until execution of a contractual agreement.

3.7 Recipient Obligation to Inform Itself

The Recipient must apply its own care and conduct its own investigation and analysis regarding any information contained in the RfP document and the meaning and impact of that information.

3.8 Evaluation of Offers

The issuance of RFP document is merely an invitation to offer and must not be construed as any agreement or contract or arrangement nor would it be construed as any investigation or review carried out by a Recipient. The Recipient unconditionally acknowledges by submitting its response to this RFP document that it has not relied on any idea, information, statement, representation, or warranty given in this RFP document.

3.9 Acceptance of Selection Process

Each Recipient / Respondent having responded to this RfP acknowledges to have read, understood and accepts the selection & evaluation process mentioned in this RfP document. The Recipient / Respondent ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RfP.

3.10 Errors and Omissions

Each Recipient should notify SIDBI of any error, fault, omission, or discrepancy found in this RFP document but not later than twelve days prior to the due date for lodgment of Response to RFP.

3.11 Acceptance of Terms

Recipient will, by responding to SIDBI for RfP, be deemed to have accepted the terms of this Introduction and Disclaimer.

3.12 Requests for Proposal

3.12.1 Recipients are required to direct all communications related to this RfP, through the Nominated Point of Contact, to following SIDBI Officials:

Contact Person	Debashish Das	Narender Kumar	Rajesh Joshi
Designation	AM(Systems)	AGM (Systems)	DGM (Systems)
Email ID	debashishd@sidbi.in	narender@sidbi.in	rjoshi@sidbi.in
Telephone No.	022-67221480	022-67531238	022-67531251

3.12.2 SIDBI may, in its absolute discretion, seek additional information or material from any Respondents after the RfP closes and all such information and material provided must be taken to form part of that Respondent's response.

3.12.3 Respondents should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RfP could be conveyed promptly.

3.12.4 If SIDBI, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then SIDBI reserves the right to communicate such response to all Respondents.

3.12.5 SIDBI may, in its absolute discretion, engage in discussion with any Respondent (or simultaneously with more than one Respondent) after the RfP closes to improve or clarify any response.

3.13 Notification

SIDBI will notify all short-listed Respondents in writing or by mail as soon as practicable about the outcome of their RfP. SIDBI is not obliged to provide any reasons for any such acceptance or rejection.

❄ ❄ ❄ ❄ ❄ ❄

4. RfP Response

4.1 Tender Cost / Bid Price

1. Non-refundable Tender Cost as specified in **"Critical Information"** section by way of Banker's Cheque / Demand Draft / Pay Order drawn on a scheduled commercial bank, favouring **"Small Industries Development Bank of India"**, payable at Mumbai must be submitted separately along with RFP response.

   Alternatively, Tender Cost may also be deposited directly in following SIDBI's Bank A/C and copy of e-receipt should be submitted along with RfP Response. SIDBI's Bank A/C Details are as under:

Account Name	Small Industries Development Bank of India
Bank	State Bank of India
Branch	Bandra Kurla Complex, Mumbai - 400051
Type of Account	Current Account
A/C No.	37823159064
IFSC Code	SBIN0004380

4.2 Earnest Money Deposit (EMD)

All the responses must be accompanied by a refundable interest free security deposit. Details of the EMD are given in **RFP Section 8.8**.

4.3 RFP closing date

RFP Response should be received by SIDBI not later than the time mentioned in **'Critical Information'** section above, at the defined address of SIDBI Office premises.

4.4 RfP Validity Period

The Bids must remain valid and open for evaluation according to their terms for a period of **six (6) months** from the last date of the submission of bids.

4.5 Late RFP Policy

Responses received after the due date / time would be considered late and may not be accepted or opened. Late received bids shall be returned un-opened **within 02 weeks from the bid submission date.**

4.6 Receiving of RFP Response

Receiving of RFP response will be recorded by SIDBI in a 'Tender Receiving Register' kept for the purpose upon receiving the RFP response. The submission of the response should be in the format outlined in this RFP and should be submitted preferably through hand delivery. If the submission to this RFP does not include all the documents and information required or is incomplete or submission is through Fax mode, the RFP is liable to be summarily rejected. All submissions, including any accompanying documents, will become the property of Bank. The Recipient shall be deemed to have licensed, and granted all rights to the Bank to reproduce the whole or any portion of their submission for the purpose of evaluation and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right of the Recipient that may subsist in the submission or accompanying documents.

4.7 Requests for information

1. Respondents are required to direct all communications for any clarification related to this RFP, to the designated Bank officials and must communicate the same in writing by the time mentioned in **'Critical Information'** section above. No query / clarification would be entertained over phone.
2. All queries relating to the RFP, technical or otherwise, must be in writing only and may be sent via email. The Bank will try to reply, without any obligation in respect thereof, every reasonable query raised by the Recipients in the manner specified. However, the Bank will not answer any communication reaching the bank later than the time stipulated for the purpose.
3. The Bank may in its absolute discretion seek, but under no obligation to seek, additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent's response. Respondents should invariably provide details of their email address as responses to queries will be provided to all Respondents via email.
4. The Bank may in its sole and absolute discretion engage in discussion with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to clarify any response.

4.8 Pre-Bid Meeting

1. The Bank shall hold a pre-bid meeting on the date and time mentioned in '**Critical Information**' section above. Purpose of the meeting would be to bring utmost clarity on the scope of work and terms of the RFP being floated. The Bidders are expected to use the platform to have all their queries answered. No query will be entertained after the pre-bid meeting.
2. It would be the responsibility of the Bidder's representatives (max. two persons per bidder) to be present at the venue of the meeting.
3. In view of the on-going COVID-19 pandemic, the Bank may decide to conduct on-line pre-bid meeting using Microsoft Team/ Skype for Business. Accordingly, while sending pre-bid queries to the designated Bank officials, details viz. Name, mobile number and e-mail id of the bidder's representatives who would be attending the pre-bid meeting, should be mentioned. In case the pre-bid meeting is held on-line, meeting invite shall

be sent one day prior only to the bidder's representatives whose details have been received by the Bank.

4. In case some bidder does not receive the meeting invite, it would be bidder's responsibility to get in touch with designated Bank officials to get the meeting invite.
5. Clarification sought by bidders should be made in writing (Letter/E-mail etc.) and submitted on or before the date as indicated in the **'Critical Information'** Section. Bank has discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.
6. The text of the clarifications asked (without identifying the source of enquiry) and the response given by the Bank, together with amendment to the bidding document, if any, will be posted on the Bank's website ( ) and Central Public Procurement Portal (CPPP) within 05 working days of the pre-bid meeting. It would be responsibility of the bidder to check the websites before final submission of bids.
7. If SIDBI, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then SIDBI reserves the right to communicate such response to all Respondents.

4.9 Disqualification

Any form of canvassing/ lobbying/ influence/ query regarding short listing, status etc. will result in a disqualification.

4.10 Selection process

Successful Bidder will be selected through three stage bid evaluation process:

[A]. Minimum Eligibility Bid evaluation

[B]. Technical Bid evaluation

[C]. Commercial Bid evaluation.

4.11 Details of Bids to be Submitted

1. Bidders are required to submit their responses in THREE envelopes, with contents of each as under:

Envelope #	Bid Contents	No. of Copies	Label of Envelope
I	**Minimum Eligibility Bid** i. DDs / Instruments towards bid price ii. DDs/ Instruments towards Earnest Money Deposit **(EMD) OR** Bank guarantee towards EMD as per format prescribed in **Annexure-XIV**. iii. Bid Forwarding letter as per format prescribed in **Annexure-I**	Hardcopy – 1 Copy A CD /Pen-drive -A	**"Minimum Eligibility"** **Datacentre & DR Site Infrastructure Managed Services** **RfP No. 400/2021/1619/BYO /ITV dated March 16, 2021**

Envelope #	Bid Contents	No. of Copies	Label of Envelope
	iv. General Information about the bidder as per format prescribed in **Annexure-II** v. Response to Minimum Eligibility Criteria as per format prescribed in **Annexure-III** vi. Declaration regarding clean track record, as per format prescribed in **Annexure-IV** vii. Conformity of Hardcopies in **Annexure-V** viii. Statement of deviations as per format prescribed in **Annexure-VI** ix. Letter of competence as per format prescribed in **Annexure-VII** x. Power of Attorney as per format prescribed in **Annexure-VIII** xi. Letter of Conformity as per format prescribed in **Annexure-IX** xii. Non-Disclosure Agreement as per **Annexure-XII** xiii. Bank Mandate Form as per format prescribed in **Annexure-XIII**. xiv. Pre-Contract Integrity Pact as per format **Annexure-XVI**	containing Editable Softcopy – 1 Copy	
II	**Technical Bid** i. Details and corresponding documents as required for all the Technical Parameters stipulated under **Section 10.2.2** ii. Resource deployment plan as per format prescribed in **Annexure-X** iii. Masked Commercial bid as per format prescribed in **Annexure-XVII**	Hardcopy – 1 Copy A CD /Pen-drive - B containing Editable Softcopy – 1 Copy	**"Technical Bid"** **Datacentre & DR Site Infrastructure Managed Services <u>RfP No.</u> 400/2021/1619/BYO /ITV dated March 16, 2021**
III	**Commercial Bid** i. Commercial Bid Forwarding letter as per format prescribed in **Annexure-XI** ii. Response to Commercial Bid as per format prescribed in **Annexure-XVII**	Hardcopy – 1 Copy	**"Commercial Bid"** **Datacentre & DR Site Infrastructure Managed Services <u>RfP No.</u> 400/2021/1619/BYO /ITV dated March 16, 2021**

2. Above mentioned three separately sealed sub-envelopes should be put together in another master sealed envelope super-scribing **"Datacentre & DR Site Infrastructure Managed Services, RfP No. 400/2021/1619/BYO/ITV dated March 16, 2021".**

3. All the individual envelopes must be super-scribed with the following information as well:

i. Name of the bidder, Contact Number and mail id.
ii. Bids should be enclosed with all relevant documentary proofs / certificates duly sealed and signed.
iii. Envelope I, II should also contain softcopy of respective response documents, copied in a DVD / Pen-drive.

4.12 Pre-contract Integrity Pact (IP) and Independent External Monitor (IEM)

1. IP is an agreement between the prospective vendors / bidders and the buyer committing the persons / officials of both the parties not to exercise any corrupt influence on any aspect of the contract.
2. The bidder has to submit signed Pre-contract Integrity Pact (IP) as per the format at **Annexure-XVI** on a non-judicial stamp paper of requisite value (to be borne by the bidder) as applicable at the place of its first execution along with the minimum eligibility bid.
3. The Bidders are requested to note that in reference to the Central Vigilance Commission (CVC) Circular, Bank has appointed Shri Nageshwar Rao Koripalli, IRS(Retd.) as an Independent External Monitors (IEM) in consultation with the Central Vigilance Commission. Name and Address of the IEM are as follows:

Shri Nageshwar Rao Koripalli, IRS (Retd.)
38, The Trails, Manikonda, R. R. District
Hyderabad - 500089
Mobile : 9788919555
Email : knageshwarrao@gmail.com

4.13 Important

Bidders must take the following points into consideration during preparation and submission of bids.

1. Relevant documents must be submitted as proof wherever necessary. All the pages must be sealed and signed by the authorized signatory of the respondent.
2. Faxed copies of any submission are not acceptable and will be rejected by the Bank.
3. Responses should be concise and to the point. Submission of irrelevant documents must be avoided.
4. If the bids do not contain all the information required or is incomplete, the proposal is liable to be rejected.
5. The RfP is floated on SIDBI website **www.sidbi.in**, Central Public Procurement Portal (CPPP) at **eprocure.gov.in** and notification given in Indian Trade Journal. SIDBI reserves the right to change the dates mentioned in **'Critical Information'** section. Changes and clarification, if any, related to RfP will be posted on SIDBI website and CPPP. Bidders

must have close watch on SIDBI website and CPPP during the intervening period before submitting response to RfP.

6. The bidder cannot quote for the project in part.
7. Each bidder shall submit only one proposal.

❄ ❄ ❄ ❄ ❄ ❄

5. Background

5.1 Introduction

Small Industries Development Bank of India (SIDBI) set up on 2nd April 1990 under an Act of Indian Parliament, acts as the Principal Financial Institution for Promotion, Financing and Development of the Micro, Small and Medium Enterprise (MSME) sector as well as for co-ordination of functions of institutions engaged in similar activities.

The Bank provides its services through a network of offices located all over India. Detailed information on the functions of the Bank is provided on the website **www.sidbi.in**.

5.2 IT Infrastructure

SIDBI's IT Operations and the infrastructure is managed by Information Technology Vertical (ITV) through an in-house team of IT Officers at different levels. Management of some of the functions and application development on need basis is outsourced to 3rd party vendors. The ITV along with 3rd party vendors operates currently out of SIDBI's Lucknow, Mumbai and Chennai Offices. While the application development and application user support are primarily handled out of Lucknow Office, IT Infrastructure Management including DC and DR Site operations are handled by the teams at Mumbai and Chennai offices. However, depending on Bank's administrative convenience, teams/ roles at respective locations as mentioned here may be re-located to any other location(s) during the contract period.

A brief on IT Infrastructure is given in following sections:

5.2.1 Datacentre (DC) & Disaster Recovery (DR) Site

SIDBI has its Datacenter at Mumbai and DR Site at Chennai. Both DC and DR are co-located at 3rd party datacenters at respective locations. While the datacenter facilities viz. DC cage, Racks, power, UPS, cooling, humidity controls, physical security, fire and safety controls etc. are provided, managed and maintained by the Datacenter Service Provider, the IT Infrastructure items hosted inside the DC Cage viz. Servers, Storage, Network and Security devices, Backup devices, LAN/ WAN etc. are owned, managed and maintained by SIDBI or through its 3rd party managing partner(s), both at DC and DR. Bank has also taken certain number of seats at both the DC and DR for seating of on-site resources. All the applications are hosted at Datacenter and the same are accessed over SDWAN. In the event of failure of Datacenter, DR Site is activated.

5.2.2 Present IT Infrastructure

Infrastructure Type	Details of Components
Hardware	Servers (Rack & Blades with majority on Intel and few on RISC architecture), Routers, Switches, Backup Tape library, SAN Storage, Security devices, Video Conferencing End points, biometric attendance systems etc.
Operating Systems	HP-UX 11.31 v3, Windows 2008/2012/2016/2019, Linux
Virtualisation	Citrix XenApp Enterprise Edition for Application virtualization and VMWare for Server virtualization
Backend databases	Oracle 11g/ 19c in RAC (Real Application Cluster), Oracle Data guard for DR replication of archive logs, MS SQL, MySQL
Application Servers	Citrix XenApp 7.15, IBM Websphere and MQ-Series, Oracle Application Server, Oracle WebLogic
Web Server	JBoss, Apache Tomcat, IIS, IBM HTTP
Development Tools	Oracle Forms & Reports 12c, Java/JSP, IBM Domino, IBM Rational, .Net, PHP etc.
Groupware	Microsoft Office 365, IBM Domino 9
Enterprise Backup Solution	LAN/SAN based backup using Veritas Netbackup Enterprise Server 8.1.1
Office Automation	Microsoft Office 365, MS Office 2013, Unicode
Antivirus S/w	Symantec End Point Enterprise Edition Ver.14
LAN	Data Center and DR site- L3 Switch based LAN. All switches are of HP make (HPE 7904,HPE 5930, HPE 5945). In addition, few L2 switches are also used for interconnect.
WAN	SDWAN is completely managed network connecting all the locations. Primary and secondary links on wired or wireless. The entire SDWAN architecture is Any-to-Any and in case of last mile from alternate service provider NNI takes place at Datacenter and DR Site. All SDWAN devices installed at respective SIDBI locations are provided and managed by the service provider.
Network Security	NGIPS (Cisco), Firewall-Perimeter (CheckPoint 15400 in failover at DC and CheckPoint 5900 in failover at DR Site), Firewall –Core (Fortigate 3600C in failover at DC and Fortigate 1200D in failover at DR Site).
Web Gateway Security	Bluecoat ASG200 web gateway security appliance with proxy and caching, web content filtering, antimalware and antivirus, with failover both at DC and DR Site.
Link Load Balancers	Radware Alteon 5208XL at both DC & DR for termination of Internet links and distribution of in-bound and out-bound traffic to and from multiple Internet Service Provider (ISP) links

Infrastructure Type	Details of Components
Video Conferencing	• The core infrastructure (on premise) consists of Polycom DMA, RSS, MCU, Firewall Traversal, PRI gateway, Resource manager and Endpoints are mix of Polycom (HDX 8000/7000/Group 500). • Microsoft Teams/ Skype as part of subscription-based MS Office365 cloud services.
EMS Tools	• HP OpenView - Operations Manager, Network Node Manager (NNM), SM9. • HP-IMC software for management of entire switching network.
Access Gateway	Citrix Netscaler
Business Applications	Website, Intranet portal, Business Application with details as given in subsequent paragraph of this document.
Cyber Security Operations Centre (CSOC)	Various security solution as part of CSOC viz. SIEM, PIM, Anti-APT, Firewall Analyser and NAC are implemented at DC and DR. CSOC is managed by 3rd party vendor.
Microsoft Office 365	Subscription to cloud hosted on-line MS Office365 Services including Exchange on-line, OneDrive, Power Point, Teams, Skype for Business, Word, PowerPoint, Excel, Advance Threat Protection etc.

5.2.3 Details of Present IT Infrastructure

5.2.3.1 Connectivity

➢ **Wide Area Network (WAN)**

SIDBI has implemented complete managed Software Defined WAN (SDWAN) based IP MPLS VPN connecting all its locations/offices. The architecture deployed is Any-to-Any with CPE to CPE IPsec enabled for secure communication.

The scope of SDWAN service provider includes supply of CPE, IP MPLS bandwidth, configuration, troubleshooting, monitoring, maintenance etc. On-site NOC with adequate resources is setup by SDWAN service provider for monitoring and management.

The bank has also contracted IP MPLS VPN bandwidth from alternate service provider for providing redundancy at key locations/offices. At other locations, the link level redundancy is provided through broadband. The NNI happens at DC and DR.

All the links (MPLS VPN & broadband) are terminated on CPE and configured in active/active mode with distribution of traffic over the links based on QoS and policies.

The last mile connectivity at the locations is wired or wireless depending upon the feasibility of the service provider. Further, the IP MPLS VPN bandwidth contracted at the locations varies from 2Mbps to 32/64Mbps and at aggregation points (DC/DR) it is 300Mbps.

The WAN network is completely converged network, wherein data, voice and video are transmitted over the same.

- **Local Area Network (LAN)**

SIDBI has implemented IP based, wired LAN at all its locations/offices.

a) DC & DR

The core LAN at DC and DR is based on Layer-3 HPE 10Gig switches deployed in leaf-spine architecture. VLANs are created on this switches for segmentation.

Further, aggregation switches (HPE, L-3, 10Gig) are deployed for termination of WAN links, third party connectivity links (SWIFT & NPCI), P2P, connectivity to DMZ etc.

b) Mumbai, Lucknow and New Delhi Offices

Two tier switching architecture viz., aggregation and access is deployed. The aggregation switches are Layer 3 deployed in HA mode on which VLANs are created as required and access switches from each floor are connected to appropriate VLAN. The nodes in each floor are connected to respective floor access switch.

c) Other locations

The LAN is based on Layer 2 managed gigabit switches which are of HP/Aruba make and all nodes at the locations are connected to the same.

d) On all the location switches 802.1X is enabled for port-based network access control. **Radius** server is deployed in DC & DR along with NAC for posture checking & Authentication.

- **Point to Point Link**

For online log shipment / replication from DC to DR, Bank has deployed point-to-point links of requisite bandwidth taken from two service providers. The links are terminated on Aggregation (L3) switches at DC and at DR.

5.2.3.2 External Networks

SIDBI also has connectivity with third party networks like NDS (Infinet), Reuters, SWIFT, Bloomberg, NPCI etc. at both DC and DR.

NDS, Reuters and Bloomberg are standalone networks terminated at Mumbai Office. However, SIDBI is in the process of integration of the same with DC / DR network through proper security.

SWIFT and NPCI are integrated with DC and DR.

The necessary network infrastructure (Links, Routers & Switches) for the above third-party network are provided by respective service providers.

5.2.3.3 Internet

Internet at SIDBI is centralized with gateways at DC and DR and all locations access Internet over WAN with proxy Authorisation.

Bank has procured Internet bandwidth from two service providers at DC and DR Site. Internet links at both locations are terminated on link load balancers. Further, 'A' records are maintained on link load balancer for the applications hosted on-premise. The DNS at service provider contains only pointers to LLB. Further, DDOS subscription for detection and mitigation of volumetric attacks is also subscribed from respective service providers.

Web Gateway Security (WGS) appliances have been installed at both locations which acts as proxy server with content filtering, antivirus and antimalware software loaded on it. The WGS is integrated with AD for authentication. Groups are created on AD and users are made members of the group. Further, policies are added on WGS and AD groups are mapped to the same.

Currently, 2x64Mbps bandwidth at DC and 2x32Mbps bandwidth has been subscribed. However, during period of contract based on the requirements bank may upgrade bandwidth / procure additional Internet bandwidth from multiple service providers at DC and DR.

5.2.3.4 Microsoft Office365

1. Bank has subscribed to cloud hosted MS Office365 on-line applications/ services under a separate tenant.

2. Subscription to these on-line applications/ services is under different licensing models viz. E5, E3 etc. depending on users' profiles. Some of the major online application/ services SIDBI is entitled to use are Exchange on-line, OneDrive, Power Point, Teams, Skype for Business, Word, PowerPoint, Excel, Advance Threat Protection etc.

3. Currently, the user management viz. creation, deletion, enabling, disabling, updation etc. to provide access to these applications/ services is done directly on

on-cloud Azure AD. However, during the contract period, if Bank decides to implement Active Directory Federation Services (ADFS) to provide Single Sign On (SSO) for accessing Office365 applications/services using on-premise Active Directory user credentials, Service Provider shall have to implement and maintain the same along with other necessary components.

4. Besides SIDBI, domains of some other associates/ subsidiaries of SIDBI viz. CGTMSE, MUDRA and NCGTC also exists in the same tenant. Domains of more associates/ subsidiaries of SIDBI, if required, may also be added to the tenant during the contract period.

5.2.3.5 E-Mail

1. **Microsoft Exchange On-line** - SIDBI is currently using Microsoft Exchange Online cloud-based services on subscription-based model. All mailboxes viz. personnel and shared mailboxes are hosted on cloud and accessed using Outlook desktop client or browser-based Outlook Web Access (OWA) or Outlook App on mobile devices.

   Outbound mails generated by internal business applications as alerts are sent from to internal (on-premise) SMTP Servers and then transferred directly over Internet.

   Bank has also subscribed to Microsoft's Advance Threat Protection email service for all users. All inbound internet mails/ attachments/ URLs from external domains get scanned for antispam, malware and viruses.

2. **On-premise IBM Domino –** Before migrating to MS Exchange on-line in 2017, SIDBI was using on-premise implemented IBM Notes Domino for mailing system. This infrastructure is still in place and is being used for few workflow-based applications.

   Under this setup, outbound mails were sent from IBM Notes to internal SMTP and then transferred directly over Internet. External mailboxes were hosted with third party. All inbound internet mails from external domains were first received at centralized hosted mailbox, gets scanned for antispam, thereafter they were pushed to SMTP server of the Bank. On receipt, these mails were distributed on IBM Notes to respective users. Mail access over internet through web browsers, handheld devises & laptops was also enabled.

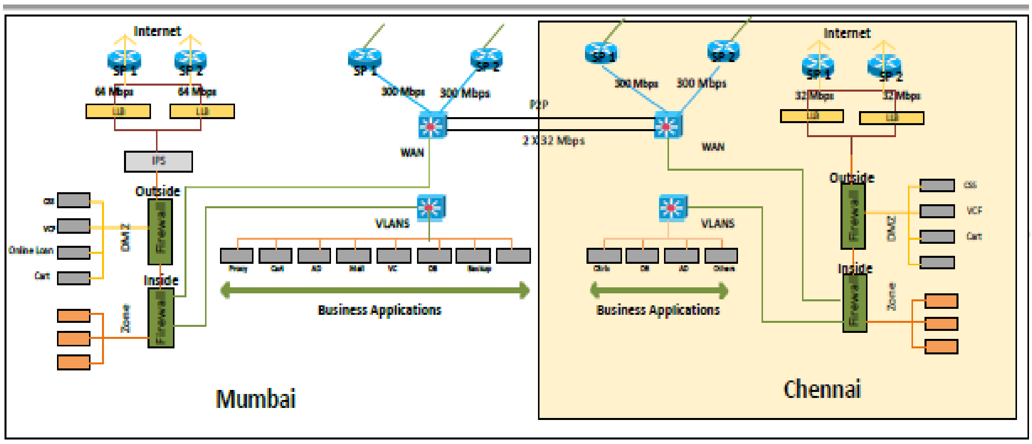
As mentioned above, though the Bank is currently using MS Exchange on-line as its mailing system, however, during the contract period if Bank decides to switch to the on-premise IBM Domino mailing system, Service Provider shall provide requisite support services on this system. **Migration of mailboxes from Exchange on-line to on-premise IBM Domino shall not be in the scope of the Service Provider.** However, management of the IBM Domino mail infrastructure both at DC and DR and providing end-user support on IBM Domino based workflow-based applications shall be in the scope of the Service Provider.

5.2.3.6 SMS facility

SIDBI has also subscribed to bulk SMS facility.

5.2.3.7 Network Architecture

High level network architecture at DC and DR is as under:



5.2.3.8 End Computing Devices

SIDBI has provided majority of its users with laptops and some users with desktop computers based on the requirement. The desktop/ laptops are installed/ configured with Microsoft Windows (7/8/10) operating system, office automation software, antivirus and basic utilities (acrobat reader etc.), clients/ apps - Citrix receiver, Outlook, MS Team, Skype, NAC etc.

However, during period of contract the bank may also implement security solutions viz., Endpoint Encryption, DLP, Asset & Patch Management solutions/agents etc., on the endpoints.

5.2.3.9 Video Conferencing (VC)

SIDBI is using following video conferencing platforms to collaborate within and outside the organization:

1. **Microsoft Office365 Teams & Skype for Business**: Bank has subscribed to Microsoft Teams and Skype for Business as part of Microsoft Office365 cloud services. Users can initiate or join MS Teams/ Skype for Business video conferences/ E-meetings from their desktops using desktop Apps or Web Apps.
2. **On-premise VC Infrastructure**: SIDBI has deployed video conferencing solution at locations/ offices. The solution is a mix of hardware/software based. The core VC infrastructure installed at Datacenter, consists of MCU, Recording, DMA, RPAD, Resource Manager, which are all of Polycom Make.

   The endpoints deployed at the locations are mix of Polycom (HDX 8000/7000/Group 500 series).

The video conferencing is carried over existing WAN and Internet (no separate network for VC is implemented).

5.2.3.10 Data Centre (DC) and DR Site Security Architecture

1 **Firewall & NIPS:**

The Security architecture deployed at DC and DR is two-layer firewall architecture i.e. internal and **perimeter**. Further, at DC Next Generation Intrusion Prevention System (NGIPS) implemented at the perimeter.

On the perimeter firewall, DMZs are created for hosting web servers, SMTP, Access Gateway etc.

Internal (Core) firewall VDOMs are created for integration of third party networks and connection to core switches. Currently, very minimal policies are maintained on the core firewall. However, during the period of contract, the ACLs created on the core switches are to be migrated to firewall.

2 **CSOC**

To secure its IT Infrastructure against cyber threats, Bank has implemented CSOC with security tools such as SIEM, PIM, NAC, Firewall Analyser, Anti-APT at DC and DR.

Implementation and management of these tools is currently in the scope of 3rd party System Integrator. In addition, providing VAPT Information and Remediation Services & Security/ Threat Intelligence Services is also in the scope of CSOC vendor. Currently, CSOC is managed by an on-site team of CSOC vendor, out of Chennai Office. Incidents raised by CSOC team are assigned to groups managing the infrastructure for resolution.

3 No separate security devices are deployed at all locations/offices. All locations access the resources hosted at DC & DR including Internet over WAN only. Locations where broadband is used as alternate link for WAN connectivity, firewall is enabled on CPE.

5.2.3.11 SSL VPN

To enable authorized staff and vendor to access applications over Internet, SIDBI has deployed SSL VPN appliances at both Data Center and DR Site.

Bank is in the process of replacing this system with full-fledged VPN solutions.

5.2.3.12 Antivirus and Operating System Patches

1 Enterprise edition of Symantec Endpoint Protection (SEP) Antivirus is deployed at datacenter and clients are installed on all the servers and end computing devices across SIDBI offices including DC and DR. The antivirus definitions are updated periodically from the antivirus server hosted at datacenter. Bank is also in the process of setting up AV server at DR for redundancy.

2 Further, WSUS server is installed in the datacenter and windows patches are periodically updated from the same to the servers including remote servers at other offices.

3 Bank is in the process of procuring/replacing and deploying end-point patching solution.

5.2.3.13 Branch/Office

All the offices are connected over MPLS VPN to Data Center and DR Site. The local LAN is connected directly to the router(s) at respective offices.

5.2.3.14 Authentication

Bank is currently using biometric as second factor for authentication. Bank is also in the process of adding MFA which will be integrated with Active Directory and applications.

Bank is also in the process of adding another multifactor authentication solution which will be integrated with Active Directory and applications.

5.2.3.15 Website

SIDBI has hosted its website with third party. Maintenance of the website including Content management is also outsourced.

5.2.3.16 Web Servers

SIDBI has hosted few web servers in its Datacentre and DR Site which are used by internal users and external users.

5.2.3.17 Cyber Security Operations Center (CSOC)

To secure its IT Infrastructure against cyber threats, Bank has implemented CSOC with following solution security solutions/ tools implemented at DC and DR:

1. Security Information and Event Management (SIEM)
2. Privilege Identity Management (PIM)
3. Anti-Advanced Persistent Threat (APT)
4. Firewall Analyzer
5. Network Access Control (NAC)

Implementation and management of these tools is currently in the scope of 3rd party System Integrator. In addition, providing VAPT Information and Remediation Services & Security/ Threat Intelligence Services is also in the scope of CSOC vendor. Currently, CSOC is managed by an on-site team of CSOC vendor, out of Chennai Office. Service provider will be required to implement the advisories & recommendations issued by CSOC team, in time bound manner.

5.2.4 Business Applications

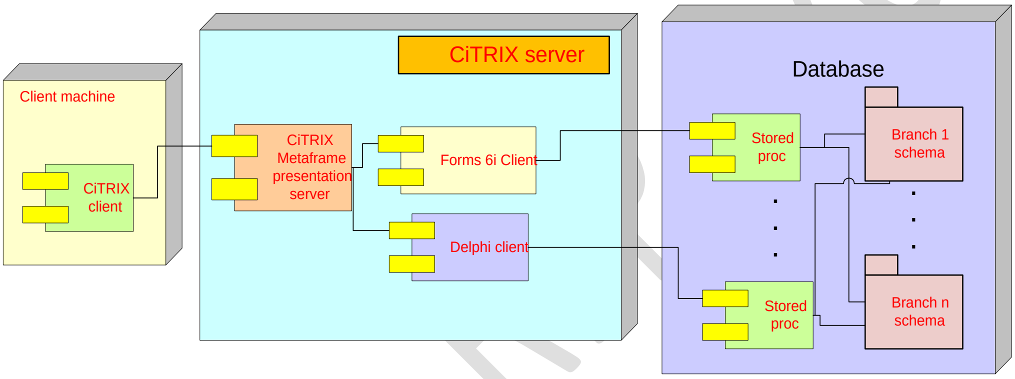
The application development, maintenance and support is done in-house and/ or outsourced on need basis. Most of the in-house applications have been developed (or ported to) in Oracle forms 12c and are being used with oracle 11g/19c databases. Few applications have been developed on Java platform. SIDBI has also purchased and implemented software for some specific operations, which use different technology. Few applications are deployed using .NET. Also, some workflow-based applications have been developed using IBM Domino.

All the applications have been deployed centrally at the Data Center using Citrix XenApp and Web Servers. Applications are accessed over WAN using Citrix web client (Citrix Receiver) or Web-browser. The client machines need to have Citrix web client Citrix Receiver) and J-Initiator (Java utility) installed to access the applications. Most of the application servers are configured in load balancing mode. There is sufficient level of clustering build at the application level for Citrix and Web Application servers as well. The central deployment of the applications allows for easy deployment of the new releases and patches. Application access over internet is enabled for selected applications for few customers and Bank's officers (on need basis), using Citrix Access Gateway.

An indicative list of applications is given in **Appendix -VII**

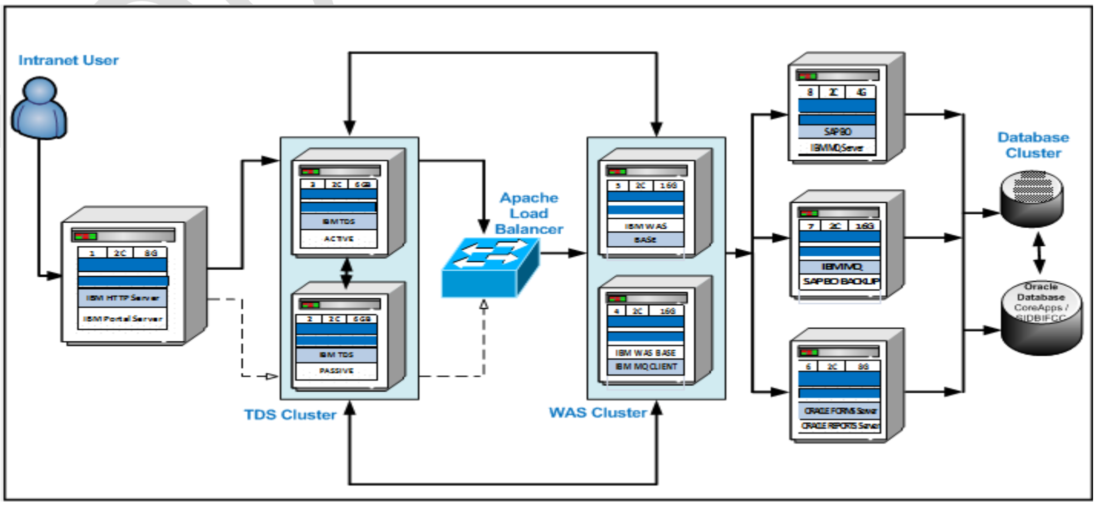
5.2.4.1 Architecture – Citrix based Application

A schematic diagram of Citrix based application deployment at SIDBI is shown below.



5.2.4.2 Architecture – Web-based Application deployment

A schematic diagram of Web-based application is at SIDBI is shown below



5.2.4.3 Integration/ Interface between Applications

1. To provide required functionality and to reduce redundancy, point to point integration among various in-house application(s) & products have been implemented using Oracle Database and IBM MQ Series.
2. Further, various on-premises applications are integrated with other on-premises / external / Cloud based applications through API / Webservices. Some of the Business applications are also having provisions to interact with Regulatory Bodies / NSDL / UIDAI etc. through API (Request / Response model).

5.2.5 Disaster Recovery

The Disaster recovery site is co-located at 3rd party Datacenter at Chennai and is the same has been configured to ensure business continuity.

5.3 Present IT Infrastructure Management

SIDBI has outsourced management of its IT Infrastructure at DC, DR and Application Support, to an external service provider through on-site resource deployment service delivery model till October 31, 2021. Broad Scope of the project includes:

1. Project Management and Governance
2. Delivery of services based on ITIL framework
3. Transition Management
4. Data Center & DR Site Managed Services
5. AMC Services for hardware items at DC and DR
6. Business applications Support
7. Management of middleware software tools on which business applications are deployed
8. Installation, Configuration, administration, customization, upgrade/patch/new release deployment, optimum utilization of the Enterprise Management System (EMS) tools.
9. Reporting & Documentation

IT Infrastructure Management Cell (IIMC) at SIDBI, Mumbai office has been setup. The IIMC Team comprises of a Program Manager, resource personnel with requisite skill sets in the respective support areas viz. Server Administration, Database Administration, Network and Security Administration (LAN & WAN), Mail administration, and Backup & Storage administration, Middleware tools Administrations, EMS Tools Administration, Application Support, Vendor Management etc. Service delivery and management is being done as per the IT Infrastructure Library (ITIL) framework.

SIDBI has implemented below mentioned Microfocus (HP) – EMS tools:

- **Microfocus (HP - Enterprise Monitoring Tools)**
  Service Manager 9 (Help Desk)
  Network Monitoring – (NNMi -9.20)
  Operations Manager : Version 9.0

Category wise/ location wise details of existing IT infrastructure are separately provided in **Appendices I - IX** in this document.

5.4 Ongoing IT Project - Summary

All news projects are separate initiatives. However, the expected impact / services required from Service provider are mentioned below.

5.4.1 IT Security

Security Roadmap: In the current FY, SIDBI would be strengthening the security by implementation of Endpoint Encryption, Multifactor Authentication, Database Activity Monitoring, File Integrity Monitoring and Asset and Patch Management Solution.
Further, during period of contract, the bank may also implement full-fledged VPN for remote access, Data Leakage Prevention (DLP), Identity and Access Management (IDAM) etc., to strengthen its security posture.

In addition to this, SIDBI may also implement various security measures time to time as recommended by regulators and Bank's requirements.

Impact: The vendor deployed engineer for management of security should have good understanding/ knowledge of various security measures as specified above. The engineer should associate with the security solution vendors shortlisted by SIDBI during installation/configuration/ management.

Respective teams of the selected service provider would be required to facilitate and carry out necessary activities including vendor co-ordination towards installation, commissioning and successful operationalization of the new / existing infrastructure items and optimally rearrange/ allocate/ re-allocate the resources in DC, DR or at any other office.

5.4.2 IT Procurement (DC/DR/ Branches)

As and when required SIDBI undertakes procurement of various IT Infrastructure item viz. Servers, Software, Backup devices, Storage, Network and Security devices, network/ internet bandwidth etc. at Data Center, DR Site and various offices to add/ upgrade the new items or replace the existing items getting phased out.

Respective teams of the selected service provider would be required to facilitate and carry out necessary activities including vendor co-ordination towards installation, commissioning and successful operationalization of the new / existing infrastructure items and optimally rearrange/ allocate/ re-allocate the resources in DC, DR or at any other office. However, network engineers have to coordinate during installation for providing / assigning management IP, testing, getting hardware integrated with existing LAN/WAN etc.

5.4.3 Outsourcing of End-user Computing Device Management – FM Support –

SIDBI has outsourced Facility Management of end user computing devices. The project scope cover outsourcing of FM Services of end user computing devices (i.e. Desktop Computer/PC, Laptop, Printer, Scanner, Switches, VC Equipment, UPS, Projectors, external HDD,CD-Writer, Finger Print device, iPad, Tablet & other IT smart devices), AMC and VC management services at all SIDBI locations.

The selected service provider under this RfP, will be required to ensure close coordination with FM Support service provider to ensure optimal service level. All the issues, wherever the interface is required with FM support service provider, needs to be supported & resolved with mutual discussion and as advised by SIDBI.

❄ ❄ ❄ ❄ ❄ ❄

6. Project Scope

6.1 Objective

SIDBI intends to go for end-to-end outsourcing of its IT infrastructure management for a period of 05 years on TCO basis with the following objectives and envisaged outcomes that the Service Provider has to ensure throughout the contract period.

1. Establish effective and efficient Infrastructure monitoring & management practices to ensure reliability, availability, quality of services and security of the Information systems.
2. Help the bank to focus on the core business activities, service delivery to its customers & administration.
3. Help the bank in freeing from the problems relating to vendor management, infrastructure, and security and performance management.
4. Incorporate/adhere the security and Interoperability guidelines issued by the Bank during the course of the contract.
5. Ensure compliance to the audits and the observations of regulatory & statutory bodies and other internal/ external audit teams/ agencies.
6. Ensure innovative use of available technologies to effectively improve 'Return on Investment' on continuous basis by improving response time and productivity for the business of the Bank.
7. Carry-out effective IT infrastructure, Applications support and tools management as per the detailed scope defined in this RfP document.
8. Enhance reliability & security of Information Systems through centralized management of IT Infrastructure adopting the necessary measures and practices like:
   a. Dynamic Scalability
   b. Centralized and Simplified Management
   c. Improved quality of Data housekeeping
   d. Lower risk of data loss
   e. Higher availability of systems and data - 24x7x365
   f. Better management of security & access control
   g. Guaranteed Service Levels
   h. Reduced administrative burden on the Bank and Information Technology Vertical (ITV) by avoiding necessity of vendor management, addressing the technical issues surrounding the IT Infrastructure.
   i. Efficient & effective management of Information Security related issues across the Bank.
   j. Availability of 'IT Infrastructure on Demand'.
   k. Aggregation of IT Infrastructure (Hardware, Storage, Networking and Software) and Management Resources.
   l. Optimal Utilization of IT Infrastructure Resources.
   m. Standardization of Systems & Improved Scalability

n. Faster Implementation cycle times
o. Stable and Predictable Physical and Technical Environment

6.2 Requisite Standard of Services

The respondent must have all the management facilities as per standard industry norms. All the processes defined for IT service delivery and support should be compliant **based on ITIL framework** of service management.

Being a financial institution, security of its internal business, systems, and data/information would be a prime concern for SIDBI while availing the services as mentioned in this document. The bidders are required to define sufficient frameworks in their proposal to mitigate the risks and also provide details of managing similar activities at other All India Banking & Financial Institutions. To ensure this, bidders are required to submit the implementation plan based on ITSM/ITIL framework as part of their technical proposal. This plan should be comprehensive enough and will include the milestones, description, timelines etc. so as to ascertain that the Services delivered to SIDBI by the bidder are:

1. As per the agreed Service levels
2. Professionally managed with domain expertise
3. Project Risks are well understood and managed

The bidder shall be responsible to implement ITSM/ITIL standards which shall promote the adoption of an integrated process approach to effectively deliver managed services to meet the Bank's expectations. The bidder shall monitor and measure processes /services and report the results and take actions to continually improve performance.

The selected service provider will be required to ensure close coordination with Facilities Management Support service provider (as described in **Section 5.4.3**) to ensure optimal service level. All the issues, wherever the interface is required with FM support service provider, needs to be supported & resolved with mutual discussion and as advised by SIDBI.

6.3 Scope at a Glance

The Bank is looking forward for the delivery of following broad area of services under the project:

1. Project Management and Governance
2. Delivery of services based on ITIL framework
3. Transition Management
4. Data Center & DR Site Managed Services
5. AMC Services
6. Business applications Support
7. Management of middleware / software tools on which business applications are deployed

8. New Implementation, Reinstallation, Configuration, Administration, Upgrade /patch /new release deployment, Performance tuning of all the software components (on existing as well as on new hardware) viz. Operating System, Database(s), Middleware Tools, Mailing Solution, Enterprise Backup Solution, Virtualization tools, Antivirus services, Webserver(s), Portal, Application Server(s) etc.
9. New Implementation, Reinstallation, Configuration, Administration, Upgrade /patch /new release deployment of all the in-house application(s) and Products.
10. Implementation, Configuration, administration, customization, upgrade /patch /new release deployment EMS tools.
11. Reporting & Documentation.

6.4 Statement of Work – Infrastructure Management

Service provider would be required to deliver all the following services and improve upon them on continuous basis throughout the project lifecycle.

Detailed scope of work for each of the high level of scope mentioned above is given below:

6.4.1 Project Management and Governance

SIDBI desires the prospective Service Provider to follow the Project Management and Governance methodology having comprehensive set of methods, practices, and techniques to support successful delivery of the proposed project to achieve the business goal of the Bank. Service Provider needs to focus at the following areas as part of its comprehensive Project Methodology.

1. Aligning the project plans with SIDBI business plans to verify that the project meets the business requirements.
2. Defining project expectations, objectives, milestones, and deliverables to reduce the risk associated with project implementation.
3. Assigning direct ownership of project deliverables and dependencies with clarity and focused approach.
4. Executing effective and flexible communication methods to bring common understanding on the status of the project.
5. Monitoring the risk plan and executing contingency plans to minimize the impact on the project.
6. Managing changes to scope which impact the schedule, quality and costs to align the changes with SIDBI priorities.
7. Tracking implementation of the project to minimize impact on SIDBI’s business continuity.
8. Continuous improvement in service delivery throughout the project lifecycle.
9. Innovative use of the available technologies to meet the expectation of Bank in achieving its business goals.

Service Provider (SP) will deploy full time Program Manager(s) at SIDBI, Mumbai who will manage the project as a whole and act as an interface between SIDBI and the Service Provider during the contract period. He will be single point of contact on behalf of service provider.

Additionally, SP will also need to put in place a strong arrangement of project governance from backend having both technical and domain expertise. It is therefore necessary that SP has a proven track record of having different towers/ verticals/ back-end teams for providing such services.

SP should provide the detailed description for project management activities as part of the proposal in response to this RFP.

Project Management/ Governance responsibilities would primarily cover the following:

a. To ensure Services Delivery and resource management.
b. To prepare project Plan, Managing the contingencies, resource management & logistics while maintaining Service delivery.
c. Risk identification and mitigation strategy.
d. To design, implement and demonstrate processes.
e. Training for its resources.
f. Customer Satisfaction rating to be measured & efforts are made for the improvement.
g. To factor resource redundancy plan for better continuity and reliability of services.
h. To create documentation for all the processes in line with quality standards.
i. Smooth taking over of the IT Infrastructure during the transition phase.
j. Implementation of tools, Application software tools (Middleware) as well as EMS tools and delivery of services must adhere to Standard Operating Procedures (SOPs), IT policy, IT security policy, Cyber Security Policy, BCM Policy, Information Security Management System (ISMS) standards or any such guidelines/ policies issued by the Bank from time to time.
k. Ensuring continuous improvement of services
l. Sharing knowledge and value addition with SIDBI IT team on continuous basis.
m. Innovative and effective use of EMS tools in delivering services
n. Overall responsibility for delivery of services as per Scope/ Statement of Work/s (SOW) and Service Level Agreement (SLA).
o. Act as a primary interface to SIDBI for all matters that can affect the baseline, schedule and cost of the project.
p. Maintain project communications with stakeholders of SIDBI.
q. Provide strategic and tactical recommendations in relation to technology related issues and technology improvement.
r. Provide escalation to Service Provider’s senior management if required.
s. Resolve deviations from the phased project plan.
t. Conduct regularly scheduled project status/ review meetings involving officials of the Service Provider and SIDBI.
u. Review and administer the Project Change Control Procedure with SIDBI Project Leader.
v. Identify and resolve problems and issues together with SIDBI Project Leader.
w. Submission of all periodic reports.
x. Preparatory activities and submission of all related information required to facilitate SIDBI in clearing invoices submitted by SP.

y. Provide necessary support and information to internal or external auditors or any other agency in carrying out audit of systems/procedures being followed in management of IT infrastructure of the bank.

z. Compliance to the audit observations, advisories from regulators, providing periodic returns statements etc., pertaining to the IT Infrastructure including Applications under the purview of this RfP.

aa. Compliance to IT Security Policies with respect to IT Infrastructure management.

6.4.2 Service Delivery Management:

Service provider will be required to use ITIL based framework for the delivery of services under the project. Accordingly, the service provider needs to submit detailed methodology including organizational setup, project management, configuration of EMS tools and transition plan which is proposed to be followed by itself for the delivery of services during the contract period using ITIL framework.

6.4.3 Forward Transition Management

SIDBI recognizes that the transition process and its effectiveness, has a significant impact on success of ongoing services. SIDBI has the following key objectives for transition:

1. Maintain steady operation of all services and maintenance of current service levels during migration of controls and responsibility from existing vendor / SIDBI to the selected Service Provider.
2. Successfully complete all activities, providing a stable platform for future improvement in service delivery and associated benefits for SIDBI Transition Deliverables.
3. **Transition period (4 weeks) tentatively starting from October 01, 2021**, shall be divided into two phases. Exact schedule will be decided with the selected bidder.
   a. **First phase** (02 weeks) will be more focused on startup activities such as resource deployment, knowledge transfer, taking over from SIDBI/current SP and transition of **"AS IS"** processes.
   b. **In Second phase** (02 weeks), Service Provider will be required to improve and optimize on **"AS IS"** processes and ensure to complete following activities:
      i. Inventory verification.
      ii. Study and analyze the existing processes with reference to ITIL framework and find out the gaps, if any.
      iii. Finalize the reporting mechanism in consultation with SIDBI.

6.4.4 Service / Help Desk

1. Shall manage SIDBI help desk using HP Service Manager tool, for the calls pertaining to work area/ domains under the purview of this RfP.
2. Shall provide "**ownership-to-resolution**" of all help desk calls, monitor and report on the progress of problem resolution, confirm resolution of the problem with the End User, and log the final resolution via the problem management system.
3. Shall record, analyze and report on calls received by the help desk, including:

   a. Call volumes and duration,
   b. Incident & Problem trends,
   c. Call resolution time.

4. Shall assign priorities to problems, queries, and requests based on the guidelines/SLA provided by SIDBI.
5. Shall monitor and report to SIDBI on 3rd party maintenance (Warranty/ AMC) vendors performance.
6. Shall monitor and report to SIDBI on SLA's with various 3rd party vendors (including WAN vendor).
7. Shall provide input to SIDBI on End User training requirements based on help desk call tracking and analysis. As part of end user support, the SP will be required to guide, handhold and resolve the support calls. However, for repeated / complex issues requiring training to the end users, the SP will be required to provide inputs / feedback to SIDBI.
8. SIDBI is having best practices for IT Service Management using ITIL Framework for Service Desk Operations. While the Service Provider would be required to maintain the existing practices, introduction of any new ITIL complaint practices and/or improvement of the existing practices would be expected from the service provider.
9. The Service Desk is currently using HP OpenView Service Manager with the following process management functionality - Help Desk Management, Change Management, Service Level Management, Call process flow, Configuration Management Database (CMDB) and Organization Management. Service provider would be required to continue to maintain these functionalities. Service Calls need to be managed using Service manager (SM).
10. Service manager has been configured and being used for the following purposes:
    a. IT infrastructure related services – Calls logged through this are handled by IT Infrastructure Management Centre (IIMC).
    b. Business Applications related services – Calls logged are handled by application support group/ desks.
    c. Service manager tool may be used by SIDBI for any other similar helpdesk / service desk operations in the Bank. In case of such requirements, service manager tool would have to be configured by the vendor.
11. Service Manager acts as a single-point-of-contact, via telephone, email and web assistance for SIDBI End Users who require assistance in the resolution of problems, concerns, query and to request Services.
12. Service Provider will provide support using skilled Service desk personnel during agreed service window. Generally the users are required to log the call through Service Center but in case of network not available or any other emergency, users can also call the centralized Service Desk to log the call and get assistance through a designated person who will provide telephone support during such hours.
13. Service Provider should implement new processes, if any, with high focus on improving first call resolution and drive productivity and proactive measures.
14. Service Desk shall provide online support / resolution of problem using tools for shadowing of user screen, taking control of remote desktops.
15. The Helpdesk module manages the complex relationships between user problems and network events and supports following features:

a. Web Interface.
b. Trouble ticketing.
c. Automatically and efficiently tracks, logs and escalates user interactions and requests.
d. End users are able to submit and check the status of reported problems via web interface.
e. Technical Specialists are able to view, change the status of the calls, reassign / transfer the call to other technical specialist through the Web Interface.
f. Able to generate various customized Service Level Reports E.g. Open Call Reports, Closed Call Reports, Problem Area / Location specific Reports, downtime reports etc.
g. Help desk offers ITIL framework-based templates that can be configured and used for the support, monitoring and tracking of any of the desired services Helpdesk allows changes, incidents, problems, service calls and templates to be related to each other.

16. Supports planned outages for activities, which require a shut-down of a node for a period of time, which results in outage of a particular Service.
17. When incidents are created either manually or automatically, helpdesk retrieves the most appropriate service level and this in turn contributes to the automatic calculation of the event resolution deadline.
18. The helpdesk allows tracking progress of an incident with well-defined timeline-based event/escalation management.
19. The Service/Helpdesk team to be deployed by the SP will generally be expected to resolve/coordinate only DC, DR & Applications support related issues of End Users.
20. Supports monitoring of the operating status of current asset inventory so that future asset needs can be effectively planned and budgeted for.
21. The escalation matrix is defined based upon Nature / Severity / Other Defined Parameters.
22. Escalation methods include E-mail Notifications using the backbone of Bank’s mailing system.
23. Service provider has to configure and update the knowledgebase, SOPs on regular basis for all the services under the scope of this project.

SIDBI’s Responsibilities

1. Help Service Provider in defining/ updating the help desk call prioritization guidelines (as a one-time activity or if necessitated during periodic reviews and/or on change in requirements), problem severity codes and escalation procedures.
2. Provide updated contact list (as a one-time activity) on periodic basis for use by help desk personnel in contacting SIDBI’s appropriate personnel for assistance/notification, as specified above.
3. Initially, communicate all SIDBI End Users on the new service delivery process, including the Hardware, Software and Services to be supported by the help desk.
4. Communicate support responsibilities and procedures to SIDBI business unit contact personnel.
5. Assist Service Provider, as requested, in the resolution of problems outside the scope of Service Provider’s responsibilities or recurring problems, which are the result of End User error.
6. Assist Service Provider in ensuring that SIDBI’s other (3rd party) vendors report problem status and resolution back to the help desk.

7. Provide an adequate level of system authority for all Hardware, Software and resources for which Service Provider has problem resolution responsibility and communications access (such as physical links, modem connections, and analog lines).
8. Assist Service Provider in the development of help desk operational procedures by providing input, review and approval of such procedures (this is expected to be a one-time activity).
9. Allow Service Provider to utilize remote access capability to remotely diagnose problems if required; and
10. Report problems and forward requests to the service desk.

Summary of Support Call

Severity/Type wise indicative number of calls being presently handled is given below. The figures given below are only indicative and may not be applicable in future. Vendor is required to make its own assessment for sizing of the Centralized Support team.

IT Infrastructure (DC / DR)	
Description	**Average / Month**
Severity 1	0
Severity 2	47
Severity 3	486
Severity 4	3629
Total Calls Received	4162
Total Yearly Calls (Last Year)	49944

Application Support	
Description	**Average / Month**
Training/Tips	6
Navigational Issue	20
Password Reset	20
Backend Correction	61
User ID / Role Assignment	321
Operational Requirement	1118
Total Calls Received	1546
Total Yearly Calls (Last Year)	18552
Number of network related incidents encounters on a monthly basis: **WAN → Approx. 80-90** **LAN → Approx. 90**	

Domain wise indicative number of calls	
Assignment Group	**Average / Month**
Change Request (All Domains)	42
Backup/Storage Support	48
EMS Tool Support	60
Treasury Support	80
Security	90
Unix Support Group	180
Network Support Group	201
Database Support Group	240
Udyami Mitra / Stand-up India	350
Office365 / Lotus Notes Support Group	375
Middleware Support	380
Wintel Support Group (Citrix, VMware, AV, AD)	570
Total Calls Received	**2616**
Total Yearly Calls (Last Year)	**31392**

6.4.4.1 Service Level Agreement (SLA) management

1. The Service Desk should include/ map the prescribed SLAs for respective services so that the SLA monitoring can be done using the HP Service Manager tool.
2. Service Desk should make it possible to register and maintain services and SLAs as well as multiple sets of support hours.
3. Service provider shall ensure to achieve the SLAs prescribed for respective services, failing which penalties as applicable shall be deducted.
4. When a call is logged in Help Desk, the available support hours should be linked to the service levels used when calculating deadlines.
5. The priority level assigned to a service call should be based on the related service level agreement and the impact.
6. It should be possible to define the services offered to the organization as well as the SLA associated with each service.
7. Service provider has to make available all the relevant reports for management of SLA.

Currently all support / service calls are being monitored in Service Manager (SM-9) and SLA is being measured using SM-9 of HP-EMS Tool. Selected bidder may have to configure the SLAs using SM-9 as per the scope. Selected service provider may be required to review and update / configure/ customize the existing installation and incorporate changes, if any.

6.4.4.2 Asset/ Inventory Management

Protecting SIDBI's investment in a computerized environment spread across multiple locations entails, firstly, knowing what those assets are and, secondly, acquiring new assets in a standard coordinated process. Service Provider should provide Asset Tracking and Management Services to this end and should coordinate and ensure the regular updation of inventory database for both software and hardware.

Service Provider's responsibilities

1. This service provides for performing asset tracking and includes performing an initial verification of inventory of Hardware and Software to validate and establish the Configuration Management Database (CMDB).
2. Service provider shall define the process for tracking Hardware and Software throughout the life cycle from procurement through disposal, including any changes performed during the useful life of the asset.
3. Record installation of all new machines, movement within site/between locations, changes in configuration/upgrade of machines.
4. Track assets, check quality, maintain utilization level.
5. Asset tagging (Labeling / Bar coding). The SP shall arrange to print the asset tags in SIDBI prescribed format and fix the tags on his own. Format of the Labels will be provided by SIDBI. No separate cost will be reimbursed for the same.
6. Ensure asset verification at DC and DR of SIDBI, once in a year, reconcile with hardware database and report to SIDBI as per Bank's guidelines.
7. Coordinate with FM Outsourcing vendor for update/reconciliation of assets in hardware database corresponding to verification of assets at various SIDBI offices under the ambit of RfP.
8. Maintain software library as part of software inventory.
9. Maintain Asset Database of IT Assets and updates the asset management database to track the move add change and Installation. The physical security of assets will be handled by SIDBI.
10. Maintain up to date inventory of all Hardware and Software assets giving information like locations, configuration details, serial number, asset, code, warranty and AMC details.
11. Track Installation of all IT equipment at DC and DR including servers, Routers switches, IDS, Firewall, Backup devices and any other IT Equipment.
12. Track Licensed software and Application, movement within site / between locations, changes in configurations etc.
13. Consolidate all license information.
14. Monitoring Warranty/AMC details to notify contract renewals (Intimate SIDBI 60 days in advance).
15. Coordinate Hardware upgrade with vendors and update the asset database.
16. Repairs and Replacement (to be assigned to Vendor Management)
17. If 'End of Service Life' (as mutually agreed between SIDBI and the Service Provider) of an asset falls in between any quarter during contract period, Service Provider will intimate SIDBI at least 3 months in advance for replacement of the same.
18. Maintain the inventory of stock in stores.

SIDBI's Responsibilities

1. Be responsible for advising Service Provider of hardware and software procurements, transfers or terminations which affect warranty and license registrations; and Notify

Service Provider of any Hardware and Software procured by SIDBI and of any changes made by SIDBI to such Hardware and Software.

2. Be responsible for End User compliance with the terms and conditions of the software licenses and manufacturers' warranty specifications.
3. Be responsible for resolving any reconciliation discrepancies with the help of Service Provider.
4. Work with Service Provider to develop and coordinate a schedule to allow Service Provider free and sufficient access to all assets when performing a physical inventory.
5. Reconciliation & acceptance of the initial inventory verification performed by vendor.

6.4.4.3 Vendor Management Services

SIDBI has various vendors (Product support/ OEM/ AMC/ Warranty) for the IT infrastructure (Software and hardware). **Service Provider** will be required to provide vendor management services to ensure proper coordination, timely support/ escalation/ resolution and seamless operations.

Service Provider's responsibilities

1. Coordinate with these vendors for support services.
2. Maintain good relations with them on behalf of SIDBI.
3. Logging calls, co-ordination and follow-up with vendors.
4. Escalation of calls to the higher levels at vendor side in case of requirement.
5. Vendors SLA tracking and monitoring with alerts and escalations (including WAN vendor)
6. AMC/ Warranty/ Support Tracking
7. Providing necessary and advance information for entering into / renewal of AMC. (However order and payment for AMC to the vendor will be made separately by SIDBI)
8. Management of assets sent for repair.
9. Maintain database of the various vendors with details like contact person, Tel. Nos., escalation matrix, and response time and resolution time commitments. Log calls with vendors Coordinate and follow up with the vendors and get the necessary spares exchanged.
10. Keep SIDBI updated on the services and performance of these third-party vendors.

SIDBI's responsibilities

1. SIDBI will provide list of all the vendors with details like contact person, Tel. Nos., escalation matrix.
2. SIDBI will provide SLA signed with individual vendors. SIDBI will advise 3rd party vendors to address the queries of Service Provider, if any.
3. SIDBI will provide to the service provider details of the 3rd party vendors as and when any contract is renewed/ entered into.

6.4.4.4 License Management

Service provider shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed in the bank. Bank is in the process of implementing Software Asset Management (SAM) Services through a 3rd party service provider. Bidder shall work closely with the SAM vendor to implement and manage the SAM process including effective license management for various OEMs/ publishers in terms of deployment vis-à-vis SIDBI's entitlement.

6.4.4.5 Miscellaneous services

Service provider will be required to provide following miscellaneous services:

1. Coordinate the disposal of hardware as per Bank's guideline issued from time to time.
2. SP is required to format / degauss the asset and also coordinate & monitor for the disposal of hardware. Necessary tool for degaussing, if required, will be provided by SIDBI.
3. In the event of shifting/ collocation of Data Center and/or DR Site by SIDBI, the service provider would be required to relocate existing resource or deploy additional resources at the new site as per the requirements. Service provider will also be required to ensure de-installation of all the hardware, supervise packing/ transportation and installation/ commissioning of equipment at new location. No extra cost will be borne by SIDBI for the same. However, packing and transportation will be arranged by SIDBI separately.
4. Suggestions / Recommendation to improve the current infrastructure architecture for better response & security.

6.4.5 Data Centre & DR Site Operations Management

Currently Bank's DC and DR Site facilities are co-located with 3rd part Datacenter Service providers at Mumbai and Chennai respectively. While the datacenter facilities viz. DC cage, Racks, power, UPS, cooling, humidity controls, physical security, fire and safety controls etc. are provided, managed and maintained by the Datacenter Service Provider, the IT Infrastructure items hosted inside the DC Cage viz. Servers, Storage, Network and Security devices, Backup devices, LAN/ WAN etc. are owned, managed and maintained by SIDBI or through its 3rd party managing partner(s), both at DC and DR. Bank has also taken certain number of seats at both the DC and DR for seating of resources on-site.

However, during the contract period, Bank may relocate the facility(ies) with some other datacenter service provider(s) or at Bank's own premises. Irrespective of the location of DC and DR, Service Provider will ensure the smooth functioning of Data Centre and Disaster Recovery (DR) Site operations throughout the contract period.

<u>Service Provider's Responsibilities</u>

1. Regularly monitor the state of environmental and power conditions inside the Datacenter and DR Site, during the service window. In case of any incident, the SP is required to inform to BMS team of the Datacenter service provider.
2. Coordinate with Service Provider/ SIDBI and 3rd party vendors to resolve any problems and issues related to the Data Center & DR Site environment conditions, power, air-conditioning, UPS, LAN, Servers, racks, fire, water seepage, dust, cleanliness, etc.
3. Guide/suggest SIDBI on best practices of the industry which might be required to be implemented at the Data Centre & DR Site.
4. Co-ordinate with SIDBI for implementing any changes that may be required towards the placement and layout of infrastructure within the Data Center & DR Site.
5. Maintenance of log registers for its own resources and visitors inside the Data Centre, if so desired by the Bank.

6. Implementation of IT Security policies and compliance thereof.
7. Adherence and maintenance of the physical access controls employed by SIDBI over and above the controls implemented by the Datacenter Service Provider.
8. Facilitating various internal & external audits e.g. statutory audit, IS Audit, Security Audit, ISO 27000 Compliance Audit, Regulatory Audits etc. and Undertaking compliance to the observations made during these audit(s).
9. Service provider is required to coordinate / facilitate and provide required details for various Audits (internal / external / regulator). The SP will be required to undertake compliance of the Audit Observations in time bound manner through SIDBI. Service provider shall also suggest and recommend infrastructural requirement, if any, to SIDBI for the purpose of giving audit compliance.

6.4.6 Server Administration/ Management

Service Provider will provide the server administration and monitoring service to keep servers stable, operating efficiently and reliably.

Service Provider's Responsibilities

1. Administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, Biometric enrollment & authentication, providing ongoing user password support, and providing administrative support for print, file, and directory services.
2. Management of the usernames, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.
3. Periodic review of privilege and redundant username/ Ids and submit report thereof.
4. Setting up and configuring servers as per configurations documents/ guidelines provided by SIDBI.
5. Installation /Upgrade / re-installation of the server operating systems and operating system utilities on existing or new servers. In case of servers with OEM/ 3rd party vendor support, service provider shall co-ordinate with respective OEM/ 3rd party vendor for the performance of such activities.
6. OS Administration including troubleshooting, hardening, patch deployment for all kind of operating systems viz. MS Windows, UNIX, Linux etc. and Virtualization software (Citrix XEN, VMware, Hypervisor etc.).
7. Managing file systems and configuration.
8. Ensure proper configuration of server parameters, operating systems administration, hardening, tuning and integration with Syslog server/ SIEM tools etc. as per the requirement of the Bank.
9. Regular backup of servers as per backup policies of SIDBI and its restoration as and when required by SIDBI with appropriate permissions. Proper check of restorability of backup media needs to be carried out periodically as defined by SIDBI. Currently, Backup & recovery is being managed using Automated Enterprise Backup Solution implemented using Veritas NetBackup & DELL Tape Library.
10. Regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, etc.
11. Regular analysis of events and logs and maintain the reports for future audit purpose.

12. Apply OS Patches and updates. Patches for windows server(s) are applied using WSUS (Microsoft utility). However, Bank may also implement alternate patch management tool during the contract period, which shall be managed by the vendor.
13. Installation / updation / Rollback of SIDBI business applications based on guidelines provided by SIDBI. Periodic installation / updation / Rollback of business applications patches as and when released by SIDBI. However, the application patch testing shall not be the responsibility of Server Administration/ Management Team.
14. Responsible for periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.
15. Logical access control of user and groups on systems.
16. Responsible for managing uptime of servers as per SLAs.
17. Take appropriate steps to comply with the audit observations made by various internal/ external auditors and timely closure/ compliance of such observations.
18. Inform to the Bank about any gaps & improvement related with security, performance, organization in the current setup.
19. Regular BIOS & firmware upgrade of Infrastructure.
20. Depending on the nature of applications deployed, Service Provider shall suggest appropriate security measures to be applied on various servers.
21. Installation and Management of other software e.g., Citrix, VMWare, IBM Domino Notes, Oracle, Application Server (Tomcat/JBoss/Oracle Application Server/IIS), IBM WebSphere application server, IBM WebSphere Portal, Visual Source Safe (VSS), Oracle WebLogic Server, Middleware tools, Web services, Security software(s), various monitoring tools/ agents as per requirement etc.
22. Installation, porting & configuring SSL certificates wherever required. SSL Certificates and/ or renewal thereof shall be provided by SIDBI.
23. Co-ordinate with SSL vendor for issuing and deployment of SSL certificates.
24. Installation, Management including installation/ re-installation, patch deployment, maintenance including Coordination with OEM / third party for Bio-metric or any other two-factor authentication system.
25. Installation, Management including installation/ re-installation, patch deployment, maintenance including coordination with OEM / third party for e-kuber, Swift, Bloomberg, Reuters, Gilts, CBLO etc. for all the software deployed for treasury operation(s) by SIDBI at any stage during the contract period.
26. Maintenance of Microsoft's Remote Desktop Services Licensing server and Citrix XenApp licensing Server for smooth functioning of Citrix environment.
27. Up-gradation & Maintenance of Microsoft's Active Directory (AD) and IBM's Tivoli Directory Services (TDS).
28. Ensuring that the Security policies & regulatory guidelines / advisories are implemented regularly.
29. Operating system hardening through appropriate configuration and patch updates.
30. Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc.

31. Periodic reviews of domain level rights and privileges.
32. Preparation/ regular updation of the new and existing Standard Operating Procedure (SOP) documents for all activities.
33. The SP will be required to install and configure the applications as per SOP provided by the Bank and maintain thereafter, so as to make applications available for usage by the Bank. Wherever SOP is not available, SP will be required to prepare and maintain it. The SP will also be required to coordinate / seek support, if required, for installation of third-party applications.
34. It may be noted that the SOP prepared/ updated for respective domains are reviewed and approved by Bank's Chief Information Security Officer (CISO) on annual basis.

SIDBI's Responsibilities

1. SIDBI authorized personnel will request for addition and deletion of users, request for change/ modification in password and for privileges. All changes will be routed through authorized personnel of SIDBI / Support desk.
2. Providing various policy documents.
3. SIDBI to provide sitting space, Desktops, network printers, Internet connectivity, telephone / fax access, etc.
4. Define and provide SIDBI backup & security policy and procedures to Service Provider, including access controls and Server backup and restore requirements.
5. Providing existing SOP and configuration documents.

6.4.7 Database Administration (DBA) Services

Service Provider will provide Database administration services including performance monitoring, performance tuning/ optimization, predictive maintenance of table spaces, log files etc. as also administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support.

Placed below is the list of databases(s) from various OEM, being used in SIDBI, along with their purpose. Going forward, based on Bank's requirements database type(s) and number of instances may vary.

Database	Purpose / No. of Instances (approx.)
Oracle Database	**15+** (production & Development / UAT environment)
MS SQL	**5+** (BALM, Board Pac, EMS Tools)
IBM DB2	IBM Tivoli Directory Services (TDS)
MySQL	Web facing Application

Service Provider's Responsibilities

1. End-to-end management and pro-active monitoring of databases on an ongoing basis to ensure smooth functioning of the same.
2. Management of changes to databases schema, disk space, storage, user roles.
3. Conduct code and configuration reviews to provide tuning inputs to the Information Technology Vertical and its Application Development Groups in order to improve the application/ database performance or resolve bottlenecks, if any. The code refers to the code written in the back-end procedures/ packages in Database. The DBA will be required

to review the code purely in terms of performance and syntax and not in terms of business logic.

4. Performance monitoring and tuning of the databases on regular basis including, preventive maintenance of the databases.
5. Management of database upgrade or patch upgrade as and when required with minimal downtime.
6. Regular backups for all databases in accordance with the backup and archive policies of the bank. Also conduct recovery/ restoration whenever required with appropriate permissions.
7. The DBA services shall be required for all the existing and new, production, development or test database, created during the contract period at Data Center and DR Site.
8. Installation / re-installation, configuration of Oracle software (or any other Database software) on Windows, HP Unix, Linux or on any other platform deployed by SIDBI during the contract period.
9. Create and maintain database required for development, testing and production environments.
10. Upgradation of Oracle (or any other Database software) database versions, patches etc. as decided by SIDBI.
11. Plan for changes in the size of databases due to business growth and project implementation based on information supplied by SIDBI and reviewing plans with SIDBI on a regular basis for comment and approval.
12. Performing database shutdowns and restarts, as necessary.
13. Undertake tasks including managing changes to database schema, disk space, storage, user roles and privileges as per SIDBI’s requirement and maintain security as per SIDBI’s IT security policy.
14. Performing reorganizations to optimize performance as and when required.
15. Maintaining the databases to meet performance standards, maximize efficiency and minimize outages, as necessary and proactively reviewing database logs and alerts and taking appropriate actions.
16. Maintaining, updating, and implementing database archive processes and procedures to recover from an outage or corruption in a timely manner, to meet the standards as per SIDBI's Business Continuity Plan (BCP) and business requirements.
17. Proactively providing capacity planning to prevent situations caused by lack of capacity (for example, dataset or table space capacity events, full log files etc.).
18. Setting and tuning system parameters for optimum database response and functions.
19. Provide performance monitoring and tuning services on the server databases.
20. Building appropriate indexes, specifying large enough buffers and caches, aligning the database implementation with IT infrastructure, monitoring databases and applications, reorganizing databases, etc.
21. Developing, documenting and maintaining physical database standards and procedures.
22. Manage database upgrade or patch upgrade as and when required with minimal downtime.
23. Backup and restoration of databases as per bank’s backup policy.
24. Synchronization of database at DR site (Standby Database) with that of production database as per prevalent DR Policy of SIDBI.

25. Maintaining Oracle 11g and higher (as and when upgraded) databases with RAC and ASM in high availability.
26. Management of RAC with Cluster Manager, instance monitoring/tuning, instance failover and recovery as well as cluster interconnects.
27. Perform general technical trouble shooting and give consultation to application development teams of SIDBI.
28. Deploying patches / releases / scripts/ ad-hoc reports for applications (In-house / products) as advised by SIDBI team.
29. Help application development teams in troubleshooting of Oracle specific (technical) errors/ issues and SQL tuning. However, errors due to business logic or data problem shall not come under the DBA role.
30. Log support cases as necessary and effectively work with Oracle Corporation (OEM/ database service support provider).
31. Maintaining databases on a Storage Area Network (SAN) utilizing disk storage from various vendors.
32. Troubleshoots with problems regarding the databases, applications and development tools etc.
33. Administer all database objects, including tables, clusters, indexes, views, sequences, packages and procedures.
34. Performance of all database related activities for implementation and maintenance of application software.
35. Providing timely compliance to the audit observations related to Databases Infrastructure as observed during various internal/ external audits.
36. Database License management as per OEM policies vis-à-vis actual deployment.
37. Updation and maintenance of SOPs.
38. Co-ordination with respective vendor for integration of Database Activity Monitoring (DAM) tool on various Database instances.

SIDBI's Responsibilities

1. Providing necessary license details along with necessary ID & Password for raising TAR with Oracle Corporation.
2. Providing existing SOPs and necessary policy documents.

6.4.8 Server Virtualization Services

Service Provider's Responsibilities

1. Installation/ re-installation, Configuration, management of Server Virtualization software.
2. Currently, SIDBI is using Citrix XenApp Enterprise Edition for Application virtualization and VMWare for server virtualization. During contract period SIDBI may install /procure any other Server virtualization product which also needs to be managed.
3. Creation, configuration and resource allocation of guest machines (VMs) on the host servers as per bank's requirements.
4. Deployment of OS, security patches, anti-virus and applications on the VMs.

5. Allocation of Logical Unit Numbers (LUNs) to VMs from SAN or any other storage box provided by SIDBI.
6. Ensure optimum performance and high availability of VMs making use of critical features of virtualization viz. VMotion, High availability, Dynamic workload management, dynamic provisioning services etc.
7. Backup and restoration of host server and VMs as per bank's backup policy.
8. Conduct regular internal audits of all deployments at Data Center and DR Site to identify the security gaps and improvement in current setup. Finding/ recommendations, if any, may be submitted SIDBI.
9. Providing timely compliance to the audit observations as observed during various internal/ external audits.
10. License management as per OEM policies vis-à-vis actual deployment.
11. Preparation of the new and updation of the existing Standard Operating Procedure (SOP) documents.

SIDBI's Responsibilities

1. Providing necessary hardware, software, licenses and media.
2. Providing existing relevant SOPs and policy documents.

6.4.9 Citrix Administration Services

Service Provider's Responsibilities

1. Installation/ re-installation/ upgradation and Configuration of Citrix servers as per SIDBI guidelines including OS installation.
2. Installation and configuration of Citrix Products currently being used, or higher version or any other product acquired during the contract period.
3. Installation and/ or deployment of patches, upgrades, feature releases and service packs released by Citrix for Citrix products in use in SIDBI.
4. Configuring and making use of all the features which could ease the administration, enhance security and increase end-user productivity.
5. User management and defining of user policies using various management consoles.
6. Configuration and maintenance of citrix license server and backup license server.
7. Maintenance of licenses on-line at MyCitrix.com and advising SIDBI well in advance on the CSA (Citrix Subscription Advantage) renewal of different license as and when getting due (minimum 60 days in advance).
8. Resolving the Issues related to the following:
   a. Citrix Data Store.
   b. Terminal Services.
   c. Citrix/ MS Licensing issues.
   d. Resource manager database and reporting issues.
   e. Windows OS related issues on Citrix Servers.
   f. Fine tuning of Citrix Server farm from time to time.
   g. Citrix Servers health checkup on regular basis and review of logs.
   h. Liaison with Citrix Systems India Pvt. Ltd. for any support requirements within the purview of CSA.

9. Implementation/ deployment of in-house or third party developed applications on Citrix servers and resolving the issues, if any, with the help of application teams and/ or third-party vendors.
10. Configuration, publishing, optimization and load balancing of applications.
11. Resolution of citrix client related problems reported by remote users like issues related to connectivity, client reinstallation, printing, local drive mapping etc.
12. Maintenance, customization of Citrix Web Interface portal.
13. Installation, configuration and integration of the Citrix NetScalar (Access Gateway) with our existing Citrix Farm, Active Directory and other Web Servers as per Bank's requirements.
14. Implementation of the Secured Socket Layer (SSL) Certificate in Access Gateway. The certificate will be provided by the bank.
15. Installation and Configuration of the Advances Access Control (AACO) software.
16. Providing timely compliance to the audit observations related to Citrix infrastructure as observed during various internal/ external audits.
17. License management as per OEM policies vis-à-vis actual deployment.
18. Preparation of the new and updation of the existing Standard Operating Procedure (SOP) documents.

SIDBI's Responsibilities

1. Providing necessary hardware, software, licenses and media.
2. Providing existing relevant SOP and policy documents.

6.4.10 Middleware – Application Management Services

Following middleware software tools would be under the scope of end-to-end management:

Sr. No.	Product	Server/ Instances #	OEM
1	IBM - WebSphere Portal Server (WPS)	3	IBM Corporation
2	IBM - WebSphere Application Server (WAS /WAS-ND)	20	IBM Corporation
3	IBM - Tivoli Directory Services (TDS)	3	IBM Corporation
4	IBM – MQ Series (Server and Clients)	6	IBM Corporation
5	IBM DB2 Enterprise Server Edition (DB2)	3	IBM Corporation
6	IBM HTTP Server (Web Server)	4	IBM Corporation
7	SAP Business Object Reporting - Business Object Software- management	4	SAP
8	Oracle Applications Server Oracle - Forms & Reports - For Flex cube	2	Oracle Corporation
9	Oracle Forms and Report Server (Oracle WebLogic)	6	Oracle Corporation
10	Oracle HTTP Webserver	3	Oracle Corporation
11	Apache Tomcat Application Server	30	Open Source
12	Apache Web Server (Reverse Proxy)	27	Open Source
13	JBoss Application Server	2	Red Hat Support
14	Visual Source Safe	1	Microsoft
15	Moodle	2	Open Source
16	SSL Deployment		All Web server

17	XAMPP	3	Open Source
18	Microsoft IIS	7	Microsoft
19	PHP	4	Open Source
20	Angular JS and Node JS	3	Open Source

#Number of servers/ instances may change depending on the business/ infrastructure requirements.

1. Installation, Re-Installation, Configuration, Parameterization, Upgrade and Maintenance of Middleware tools.
2. Installation / updation / Rollback of SIDBI business applications based on guidelines provided by SIDBI. Periodic installation / updation / Rollback of business applications patches as and when released by SIDBI. However, the application patch testing shall not be the responsibility of Middleware Team.
3. Identification, Coordination & Resolution of Performance related issues related to Hardware / Software tools.
4. Identification and Resolution of issues faced in Interface Layer of the applications.
5. Monitoring & Reporting of Interfaces (MQ, DB Layer)
6. Coordination and Resolution of issues faced related to Integration / Interface of applications.
7. Coordination with respective OEM vendors of products for resolution of any issue faced in production environment.
8. Deployment of all the required patches for all the applications.
9. Maintenance of MS Visual Source Safe software (SIDBI is using MS VSS) for version management of Source codes of the application.
10. Identification & Resolution of Performance Issues
11. Tuning of the tools for effective and optimized performance of applications.
12. Patch deployment for all the products / applications as and when delivered by SI / OEM vendor / SIDBI Team.
13. As the tool's management requires end-to-end support, Service Provider would be required to bring support from its back-end team in case on-site resources are not able to resolve the problem.
14. DR continuity for Middleware including DR Synchronization.
15. Daily monitoring of Middleware Instances.
16. ITIL Tools - Change management, Incident Management, Problem Management and Knowledge Management for Middleware.

17. Responsible for periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

18. Inform to the Bank about any gaps & improvement related with security, performance, organization in the current setup.

19. Installation, porting & configure of SSL certificates wherever required. SSL Certificates and/ or renewal thereof shall be provided by SIDBI.

20. Co-ordinate with SSL vendor for issuing and deployment of SSL certificates.

21. Installation, Management including installation/ re-installation, patch deployment, maintenance including coordination with OEM / third party for e-kuber, Swift, Bloomberg, Reuters, Gilts, CBLO etc. for all the software deployed for treasury operation(s) by SIDBI at any stage during the contract period.

22. Preparation/ regular updation of the new and existing Standard Operating Procedure (SOP) documents for all activities.

23. The SP will be required to install and configure the applications as per SOP provided by the Bank and maintain thereafter, so as to make applications available for usage by the Bank. Wherever SOP is not available, SP will be required to prepare and maintain it. The SP will also be required to coordinate / seek support, if required, for installation of third-party applications.

24. It may be noted that the SOP prepared/ updated for respective domains are reviewed and approved by Bank's Chief Information Security Officer (CISO) on annual basis.

All the above activities are required to be performed for Production Environment, UAT / Development Environment & Disaster Recovery Site.

6.4.11 VMWare Administration Services

Service Provider's Responsibilities

1. VMWare Infrastructure Administration and management.
2. Installation and management of ESXi Servers, vSphere Client and vCenter Server.
3. Installation of security patches, functional patches and version upgrades as and when released by OEM.
4. Perform performance tuning of ESXi servers.
5. Create the datastore for storing VMs and data
6. Build and deploy Virtual Machines and use Clones, Snapshots, templates
7. Hardening of VMs as per Bank's approved SOP and policy.
8. Health Check for VMs and ESXi hosts
9. Present / Assign LUN to ESXi hosts
10. Configure HA, use Distributed Resource Scheduler (DRS), Backups, vMotion, P2V and V2V conversion.
11. Manage Host storage (SAN, NAS, iSCSI)

12. Manage and Upgrade Virtual Center
13. Manage VM's/Build/Retire
14. Manage Templates and Clusters
15. Coordination with VMWare for resolution of issues related to product
16. VM Trouble shooting.
17. Maintain compliances with Bank's security policy.
18. Coordinate with IT Security Team and other domain teams to ensure compliance to the audit observations, if any, pertaining to VMWare infrastructure.
19. Coordinate with Backup and Storage Team to ensure backup and restoration of VMs as per Backup policy.

SIDBI's Responsibilities

1. Providing necessary hardware, software, licenses and media.
2. Providing existing relevant SOPs and policy documents.
3. Providing necessary approvals.

6.4.12 Microsoft Office 365 Portal Administration

Service Provider's Responsibilities

Service Provider shall be responsible for the end-to-end administration of SIDBI's tenant on Microsoft Office365 portal. List of activities to be performed, but not limited to, is as under:

1. Maintenance of existing domains and their DNS records, including domains of Bank's subsidiaries.
2. Creating new domains on need basis.
3. User Management – creation, updation, enabling, disabling, assign/ unassign O365 licenses.
4. Configuring and administering various portal services viz. MS Office, Exchange Online, OneDrive, SharePoint, Teams/ Skype for Business, PowerBI etc. by setting various parameters and security policies as per Bank's requirement.
5. End-user support and troubleshooting of various operational and technical issues faced by users in respective services.
6. Support to Facility Management support engineers in installation/ configuration/ troubleshooting of issues related to Office365, Outlook, OneDrive, MS Team, Skype for Business etc.
7. Bulk uploading of users, license assignment, licenses removal, enabling/ disabling of specific features using PowerShell command.
8. Administering Security and Compliance in O365.
9. Spam Filtering, Connection Filtering, Content Filtering, Malware Filtering
10. Anti-Spam Policies, Impersonation Policies, Advanced Threat Protection
11. Recipient Management in Exchange Online.
12. Self Service Password Reset, SPF, DKIM, DMARC, Mail Flow, Message analysis.
13. Exchange Online Protection, Transport Rules, Data Retention and Hold
14. Azure Information Rights Management, Azure Multifactor Authentication
15. Azure Sign in logs, Azure Conditional Access Policies, Mailbox Auditing

16. GAL Segmentation in Exchange Online, Password Policies, eDiscovery, DLP.
17. Exchange Online Module for PowerShell, Azure Module for PowerShell
18. Administration of On-premise IIS SMTP servers, Local and Global mail Relays.
19. Administration of Microsoft Teams.
20. Recipient Management in Microsoft Teams.
21. Teams Meeting Policies, Guest Access, Teams Access Management to users
22. Teams Module for PowerShell
23. Sync Polices for One Drive, External and internal sharing of files and folders
24. Access management in One Drive for Business.
25. License Management of Office 365 users
26. Troubleshooting of escalated issues for Outlook client, Outlook web
27. Troubleshooting of Microsoft Teams meeting issues faced by users.
28. Troubleshooting and assistance to users for One drive for Business.
29. Creating reports/ data using PowerShell for user activities in various services.
30. Ensure proper process and approval methods are followed for O365 Operations.
31. Backup of mailbox and other user data as per SOP document and backup procedure.
32. Implementation of Active Directory Federation Services (ADFS) to provide Single Sign On (SSO) for accessing Office365 applications/services, if so desired by the Bank.
33. Creation/updating of Standard Operating Procedures.

SIDBI's Responsibilities

1. Providing necessary access and administration roles on the portal.
2. Subscription to requisite Microsoft365 Services/ licenses.
3. Providing relevant SOPs and policy documents.
4. Providing necessary approvals.

6.4.13 Mail Management

As mentioned at Section 5.2.3.5 above, Bank is currently using Microsoft Exchange on-line as the mailing system with all personal and shared mailboxes hosted on cloud. Currently, there are about **1000+** personal mailboxes and **400+** shared mailboxes. Access to shared mailboxes is provided to concerned users by giving necessary permissions on shared mailboxes and/or folders therein to the personal mail ids of these users. But number of mailboxes may vary based on the bank's requirements.

However, during the contract period Bank may switch to any other cloud-based or on-premise hosted mailing system and the same shall be managed and supported by the Service Provider.

Broad scope of work for mail management with respect to the prevailing mailing system is given below. However, in case of change in mailing system during the contract period, scope of work may undergo suitable changes depending on the nature and components of the new system.

Service Provider will provide management of the prevailing mailing system being used by SIDBI. Broadly the service shall include administration and management of user accounts, mailboxes, address book, Global Address List, specific address lists, user groups, distribution lists, backup and retrieval management etc.

Service Provider's Responsibilities

1. Mail user creation and assigning appropriate license as advised by SIDBI
2. Setting up user mailbox and applying necessary parameters and policies on the mailbox.
3. Giving necessary permissions on shared mailboxes
4. Managing mail size quota.
5. Creating and maintaining Shared mailboxes, User Groups and Distribution lists updation as and when a user is being moved from one location to another location.
6. Writing/ defining mail rules as per business requirements
7. Configuring mail connectors to manage need-based mail relay.
8. Performing mail/ message trace on need basis.
9. Carrying out bulk activities through PowerShell Scripts.
10. End-user support and troubleshooting for outlook related issue viz. login, connectivity, synchronization, client configuration etc.
11. Installation, configuration and management of on-premise SMTP Servers both at DC and DR Site.
12. Monitoring mail flow between business applications and end-users through SMTP Servers and resolving issues, if any.
13. Coordination with business application teams, Database Administrators, Middleware Teams and Network Teams for resolution of issues, if any, pertaining to mail relay through SMTP Servers.
14. Assist Facility management team in Installation, Configuration of Outlook Clients on end user devices viz. PC, laptop, Mobile, Tablets etc.
15. Provide direct support to Senior Executive of the Bank.
16. Mail Administration and Security Policy Documentation. Detailed Security Policy for email services to be provided by SIDBI.
17. Creation of new and maintenance of existing Standard Operating Procedure (SOP) documents for all the processes followed in messaging domain.
18. Monitoring and Managing Advanced Threat Protection (ATP) features like Anti-Spam, Anti-phishing etc. so as to protect SDIBI from malicious content in email attachments and files in Exchange, SharePoint, OneDrive, and Microsoft Teams.
19. Change management for changes related to messaging domain.
20. Backup and Recovery Management of mailboxes as per bank's backup policy.
21. Escalations to third party vendor / OEM for product related problems and follow up for resolution.

Following would be the added responsibilities if Bank decides to use on-premise IBM Domino Mailing system:

1. Installation and configuration of IBM Notes Servers at locations as decided by the bank from time to time.
2. Monitoring the mail routing and database replication.
3. Troubleshooting of connectivity related issue pertaining to IBM Notes Server.
4. Call Screening / logging / monitoring / escalation / resolution.
5. Problem related to disk quota.

6. Management of IBM Domino Cluster Server & synchronization with DR Site
7. Management of IBM Traveler & IBM Same Time Server
8. Management of Mail Journaling, Domino Attached & Object Storage (DAOS)
9. Setting up Disk, Mailbox & mail size quota. SIDBI to provide quota size information and approval.
10. Monitoring the effectiveness of Antivirus software installed on all the IBM Notes Domino servers and taking remedial actions in case of faults including taking up and follow up with the OEM/Support vendor.
11. Monitoring the flow of inbound/ outbound internet mails and follow up with third party vendor/ ISP to resolve issues, if any, pertaining to internet mails.
12. Assist Facility management team in Installation, Configuration of Notes Clients on end user devices viz. PC, laptop, Mobile, Tablets etc.
13. Provide known error data base and testing process.
14. Load monitoring with logs as per SIDBI guidelines.
15. Documentation for mail server and client installation and configuration.
16. Analysis of problem and its resolutions related to IBM Notes R9 (or future versions) both at server as well as client's side.
17. Support and Administration of IBM Notes Services on Servers.
18. Installation / reinstallation / Migration, upgradation and configuration of IBM Notes Domino Server, SMTP and Relay client, Cluster Server on Windows / Linux
19. Internet mail integration (integration of mail with SIDBI's domain)
20. Management of Anti-Spam software / hardware.
21. Management & configuration of SMTP & Traveler server in Demilitarized (DM) Zone.
22. Installation / upgradation / support of IBM Notes clients on desktops.
23. Monitoring the health and availability of the IBM Notes services.
24. Maintenance of security and authentication of users.
25. Recertification of Expired ids.
26. Create, Delete & Modify users & groups. (With proper authorization)
27. Change management for any email or domain user request.
28. Backup and Recovery Management of Mail Servers and mailboxes as per bank's backup policy.
29. Policy implementation and management on server / client.
30. Sizing of mailboxes, maintenance of connection documents etc.
31. Troubleshooting problems related to IBM Notes and domain.
32. Optimization of configuration of Mail Server over WAN.
33. Implementation of external Digital certificate and & integration with mail ID.
34. Creation/ Deletion/Renaming/Re-certification of Users & User ID management.
35. Transfer of user-id/ mailboxes as and when a user is being moved from one location to another location.
36. Management of Anti-Virus Tool on mail gateway.
37. Verification for Cluster Server configuration/updation/synchronization.
38. Periodic review and reporting of logs and corrective action.

SIDBI's Responsibilities

1. To provide existing messaging SOPs
2. To provide all requisite software and license details.
3. Request for user addition and deletion and request for change/ modification in privileges will be forwarded through proper channel.
4. For E-mail messaging, File & print and all other server services, define and provide to Service Provider policy for:
   a. size and age of mailboxes to be maintained, and
   b. Mail routing schedules and priorities.
   c. User Id creation.
   d. E-mail policy and changes therein from time to time.
   e. Necessary approvals

6.4.14 Anti- Virus (AV) Management

SIDBI is currently using Symantec End Point (SEP) Antivirus software installed on Servers and desktops across SIDBI. The deployment of AV software has been done using Hub-Spoke model. Datacenter acts as the major hub from where the software upgrades and virus definition files are pushed to other hubs and nodes.

AV management service includes virus detection, eradication, logon administration, synchronization across servers / PCs / Laptops and support for required security classifications. The scope of services is applicable to all the nodes, all current and future versions of the AV software.

Service Provider's Responsibilities

1. Support for virus control and loading of antivirus patches/ signatures as and when available.
2. Installation / upgrade / support of Antivirus software clients on servers.
3. Installation / upgrade / support of Antivirus software on desktop / laptop shall be under the scope of Facility Management Service (FMS) vendor. However, all upgrades and virus definitions will be pushed from central server to the hub nodes by DC team. In case of any issue in implementation of upgrades and virus definitions on endpoints, DC team will be required to resolve jointly with FMS team.
4. Daily monitoring of all endpoints through SEP server dashboard and ensure that all the servers/ desktops are updated with latest virus definition on real time basis.
5. Implementation policy of automatic updation of virus definition and patches.
6. Based on criticality of the service for this requirement, service provider must act on proactive basis rather than act on reactive basis.
7. Problem analysis and its resolution related to Antivirus.
8. Periodic review and reporting of logs and corrective action.
9. Register and update anti-virus tools periodically as per SIDBI's contract with the anti-virus tool vendor.
10. Must scan storage media viz. Floppy disks, CD ROM, Network Drives, pen drive etc. automatically in real-time when accessed.
11. Must scan formats supported by antivirus software.

12. Diagnose and rectify any virus, spam, worm problems, which can be fixed by the anti-virus tool.
13. Provide feedback to SIDBI on any new viruses detected or possible virus attack and take up promptly with OEM/ Support vendor for getting the vaccine and carry out the timely vaccination.
14. Provide monthly proactive and reactive performance reports.
15. Guide/suggest SIDBI on the effectiveness of anti-virus management and alternate remedial action, if any.
16. Conduct regular Internal Audits to identify the best possible solution architect for SIDBI environment so as to use resources effectively & get the same implemented with the approval of SIDBI.
17. Providing timely compliance to the audit observations related to Antivirus infrastructure as observed during various internal/ external audits.
18. Prepare and update the Standard Operating Procedure (SOP) document on the A/v deployment architecture in SIDBI.

SIDBI's Responsibilities

1. To provide AV software, license and OEM/ Support vendor details
2. Provide existing AV Management policy, if any.
3. Provide existing SOP document on the AV deployment architecture.

6.4.15 Back Up / Restore Management

SIDBI has deployed Veritas NetBackup Enterprise Server, Enterprise Backup Solution (EBS) to take care of the data backup requirements of the infrastructure (Servers, Applications, databases, Network and Security Devices, mailing solutions etc.) deployed in its Data Center and DR Site. The entire solution comprises of requisite number of licenses & agents, a master server (hosted on HP Intel Server) and a DELL ML3 Tape Library with 04 FC LTO-7 drives. The EBS is supported by a well-documented backup policy aligned with bank's business/ regulatory requirements. The EBS is ready to support LAN Free backup and bank at any stage during the contract period may decide to enable LAN Free backup by procuring requisite licenses/ hardware.

Similarly, separate EBS solution with Veritas NetBackup Enterprise Server 8.1.1 and TENDBERG Overland NEOs-T24 Backup Tape Library with 02 LTO-7 drives, is installed at DR Site.

SIDBI is having separate backup policies for its DR Site and remote offices. Backup Restore management at DR Site and remote offices will also come under the purview of this service.

Service Provider will perform backup and restore management in accordance with bank's policy and procedures for backup and restore, including performance of daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.

Backup Tape movement between DC/DR and Bank's off-site location has been outsourced to respective Datacenter Service Providers. For DC, off-site location is Bank's Mumbai Office and for DR it is Bank's Chennai Office.

Service Provider’s Responsibilities

1. Backup and restoration of Operating System, applications, databases and file system etc. in accordance with defined process / procedure / policy.
2. Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
3. Ensuring prompt execution of on-demand backups & restoration of volumes, files, database and applications whenever required by User Departments or in case of upgrades and configuration changes to the system.
4. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
5. Media management including, but not limited to, tagging, cross-referencing, storing (both on-site and off-site), logging, testing, and vaulting in fireproof cabinets.
6. Installation, re-installation, upgrade and patch deployment of the EBS Software in the event of hardware/ Software failure, OS issues, release of new version or patches by the OEM etc.
7. Performance analysis of the Backup infrastructure and rework of backup schedule for optimum utilization.
8. Generation and publishing of backup reports periodically.
9. Re-cycling of off-site tapes from the Off-site backup location as identified by the bank.
10. Coordinate with the off-site backup tape movement service provider/ courier agency and the identified nodal officer(s) at off-site locations for sending/ receiving off-site tapes.
11. Coordination for maintaining inventory of off-site tapes at respective locations i.e. DC, DR, Mumbai Office and Chennai Offices.
12. Tape/ LTO library management – loading and unloading tapes, etc.
13. Coordinating to retrieve off-site media for in the event of any disaster recovery.
14. Forecasting tape requirements and giving timely indent to concerned SIDBI Team for timely procurement of the new tapes.
15. Ensuring failed backups are restarted and completed successfully within the backup cycle.
16. Periodic Restoration Testing of the Backup and maintaining evidences thereof.
17. Interacting with Process Owners in developing / maintaining Backup & Restoration Policies / Procedures.
18. Guide/suggest SIDBI for improvement/optimization of the existing backup/restore policy.
19. Coordination with EBS hardware / software vendors for resolution of problems as per SLA.
20. Backup of local servers at DR Site and at remote offices on external media viz. LTO, CDs, Hard disk etc. as per defined backup policies. Vendor shall coordinate with local FM Support engineer at remote offices for this activity.
21. Maintain log of backup/ restoration.
22. Providing timely compliance to the audit observations related to Enterprise Backup system infrastructure as observed during various internal/ external audits.
23. Update/ Maintain Standard Operating Procedure (SOP) documents.

SIDBI’s Responsibilities

1. To provide requisite hardware, Software, licenses and OEM/ Support vendor details.
2. Provide existing backup policies pertaining to Data Center, DR Site and remote offices.

3. Provide existing SOP document on the Backup and Restoration Management.

6.4.16 Storage Administration and Management

Service Provider's Responsibilities

1. Installation and configuration of the storage system at Data Center and DR Site.
2. Management of storage environment to maintain performance at desired optimum levels.
3. Development of storage management policy, configuration and management of disk array, storage virtualization, SAN fabric / switches, NAS, tape library, etc.
4. Configuration of SAN whenever a new application is hosted in the Data Center or at DR Site. This shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.
5. Providing timely compliance to the audit observations related to storage infrastructure as observed during various internal/ external audits.
6. Preparation of Standard Operating Procedure (SoP) document for the Storage Administration.

SIDBI's Responsibilities

1. To provide requisite hardware, Software, licenses and OEM/ Support vendor details.
2. Provide existing storage management policies, if any, pertaining to Data Center, DR Site.
3. Provide necessary application architecture and deployment details as and when a new application is hosted.

6.4.17 Security Administration Services

Service Provider's Responsibilities

The primary responsibility of the Information Security Administrator (ISA) would be physical and electronic protection of data: access controls, intrusion detection, virus protection, self-audit, incident response, security engineering, Implementation and compliance to the security policies and procedures, monitoring & analysis logs of network / security devices / servers etc.

The ISA has to carry out tasks related to security devices (current and proposed to be added by Bank) independently. However, for servers, network, Middleware, Vmware, AV etc. has to coordinate with various groups (such as Windows Administrator, Unix Administrator, Citrix Administrator, Vmware Administrator, Antivirus Administrator, Network Administrator etc.) and ensure that all the devices are secured and entire SIDBI computing environment is protected.

The ISA also to carry out firewall, NGIPS administration. The administration of these device would be carried out by firewall administrators who would be reporting to ISA.

A. The primary responsibility of ISA would be:

1. SIDBI has well defined IT Security and Cyber Security Policies which are periodically reviewed and updated by the bank. The security administrator is responsible for creation & maintenance of process, procedures & guidelines for implementation and management of the IT security and Cyber Security policies. Further, the security administrator should ensure the process are followed by all the groups.

2. Continual Improvements - Analyse current security requirements and make suggestions for improvements & architectural changes based on Bank IT Security policy, Cyber Security Policy, risk perception, change in environment and Industry best practices. The improvements also involves suggestion of new solution requirements for strengthening of security.
3. Network Architecture
   a) Periodic review of high and low level network architecture diagrams being maintained by network team and ensuring the same is upto date. The network diagram should include all the components installed/terminated at DC and DR.
   b) Re-designing network architecture based on the requirements of the bank to enhance the security posture, comply to guidelines from regulators, threat scenario etc. This should be an on-going process.
   c) Defining process for IP schema management across the organisation and periodic review in coordination with network administrator.
4. Designing architecture, configuration and management of security for:
   a) Online applications and services hosted or proposed to be hosted by the Bank. The security administrator should develop process for submission of requirements by various teams, analysis of requirements, designing architecture for deployment etc.
   b) Integration with external customers/ partners and 3rd party cloud service providers using API or any other interface/ technology.
   c) Third party services, networks procured/subscribed by the bank.
5. Creation and Defining process & guidelines and ensuring the same are followed by all the groups managing the DC/DR & branches infrastructure:
   a) **Patch management** – defining policy, process & guidelines for patch management and ensuring the patches for the devices/operating systems and other software's deployed in the banks environment are regularly updated (coordination with respective groups). Ensuring emergency patches are updated on high priority by respective teams.
   b) **Upgradation** – defining policy, process, guidelines for upgradation of operating systems, databases etc., installed in the banks environment.
   c) **Hardening** - defining hardening guidelines, procedures & process for implementation of the same for all devices hosted in DC, DR and branches viz., network & security devices, operating systems, middleware, applications, webservers, endpoints etc. The hardening documents to be reviewed and updated periodically based on audit observations, incidents learning, regulatory guidelines, Industry best practices.
6. Periodic review of configuration changes carried out by respective groups. The security administrator has to take into account the Change Requests (CRs) raised, PIM log analysis etc. for carrying out the same.
7. Encryption – defining process, procedure, guidelines for implementation of encryption policy of the bank, which includes (i) Encryption of data in rest, motion and transit (ii) selection of Encryption protocols (iii) Key management. The ISA should also suggest appropriate solutions, if any, for implementation of encryption and key management.
8. Coordination with:
   a) ISMS Consultant and ISMS Auditor to ensure implementation and upkeep of ISO standard and continuation of ISO 27001 certification of the Bank.

b) IS Auditors during audits. Coordinating & guiding respective internal teams for audit compliance and closure. Security administrator would be single point of contact for the auditors. The security administrator should update the hardening & process documents, based on the observations.

c) CSOC and respective teams for incidents closure.

d) VAPT audits – reviewing the report and guiding respective teams and application development teams in closure of observations.

e) Consultant engaged by the bank for any other certification process for internal systems and processes.

f) Concerned teams/ stake holder for early resolution and restoration of services in case of any cyber/ DDoS attack and necessary disaster management.

g) Bank CISO team and other working teams for submission of returns to regulators.

h) Coordination with respective teams and third party vendors/service providers for implementation of security measures as recommended by the vendor for SWIFT, NDS and other third party services contracted by the bank.

9. The security administrator to ensure:

   a) Protecting the entire network from malicious entities such as hackers, viruses, spyware etc.

   b) Security of traffic that passes through the network.

   c) Identify threats and work to create steps to defend against them.

   d) Defend systems against unauthorized access, modification and/or destruction.

10. The security administrator to coordinate with the vendor and respective teams for Implementation / integration of various security solutions, including solution refresh at DC/DR, as and when procured by the Bank during the period of contract.
11. Respond to security breaches or other security incidents and coordinate with respective teams and OEMs in case of a new threat is observed to ensure that workaround / patch is made available for the same.
12. Guide respective working teams in implementation of security and hardening measures.
13. Alert / advise SIDBI about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.
14. Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
15. Periodic review of access management system, security of physical and digital assets, data and network security, backup and recovery etc. at DC/ DR.

B. Firewall Management Services

The firewalls deployed at DC & DR are Next Generation Firewalls with application control, intrusion prevention, advanced visibility etc. Further, the bank has also deployed Cisco NGIPS at the perimeter in DC. During the contract period, the bank may upgrade the security architecture by deploying additional firewalls & IPS, replace existing firewalls/NGIPS, enable other security modules on the existing devices etc.

In addition to the above, the bank has also deployed separate firewall for NDS connectivity at DC and DR, which are currently not integrated with DC / DR network. The management of the firewalls is also under the scope of firewall engineer.

The primary responsibilities of firewall administrator would be managing the firewalls and NGIPS under the guidance of ISA. The broad scope of work of would be as under:

1 Complete Management of NGFW firewalls and NGIPS including troubleshooting, hardening, patch deployment, upgradation of signature, policy/rule management etc.

2 Periodic review of rules created on the firewalls. Co-ordinate with CSOC team for analysis of rules using firewall analyser deployed by the bank and taking corrective measures.

3 Apply Patches, signatures and updates/upgrades as and when released by OEM.

4 Regularly monitor and maintain a log of the performance monitoring of firewall & NGIPS including but not limited to monitoring of CPU, disk space, memory utilization, I/O utilization, sessions etc.

5 Upgradation of firewall software version as and when released by the OEM in coordination with bank team and vendor.

6 Configuration and management of rules/policies based on requirement of respective teams for deployment of applications and other infrastructure.

7 VPN – creation/deletion/modification/maintenance of site-to-site VPN & client-to-site VPN based on requirements of the bank for connecting to other organisations

8 NGIPS

a) Configuration and tuning for Threat intelligence based filtering.

b) Configuration of application control and periodic review and tuning.

c) Monitoring application control and application flow through the NGIPS.

d) Periodic Signature updation.

9 Virtualisation – virtualise firewall for termination of different segments in the network.

10 DMZ – Create/delete/modify & manage DMZ.

11 Co-ordinate with CSOC team for rule analysis and taking corrective steps.

12 Regular analysis of events and logs and maintain the reports for future audit purpose.

13 Periodic backup/recovery of configuration.

14 Providing timely compliance to the audit observations related to infrastructure under management as observed during various internal/ external audits.

15 Update/ Maintain Standard Operating Procedure (SOP) documents.

SIDBI's Responsibilities

1. To provide requisite Software, licenses and OEM/ Support vendor/ Service providers/ Escalation details.
2. To provide contact details of vendors.
3. To provide necessary approval to the Change requests.
4. To provide policy, SOP, hardening documents etc., if any.
5. To provide copy of IT Security, Cyber Security policies and regulatory requirements.

6.4.18 Network Management Services

Network Management services includes management of DC, DR & other office LAN, third party networks terminated at DC & DR, Internet connectivity & link load balancers Management and coordination with SDWAN service provider for troubleshooting flow of traffic.

Network Management services includes management of DC, DR & other office LAN, third party networks terminated at DC, DR & Mumbai Office, Internet connectivity, Web Gateway Security (Proxy) & link load balancers, Management and coordination with SDWAN service provider for troubleshooting flow of traffic.

Service Provider's Responsibilities

1. **Monitoring**

   a. Monitoring of LAN at Data Center, DR Site and other locations using HPE IMC tool provided by the bank.
   b. Monitoring of the main and backup/secondary Links of third party networks other than SDWAN links and reporting.
   c. Monitoring of incoming & outgoing traffic from the network.
   d. Network capacity monitoring, including device resource utilization at DC/DR & other locations LAN, which includes third party links.

2. **Fault Management**

   a. Co-ordination, troubleshooting and resolution of WAN reachability issue, integration of WAN links etc., along with SDWAN service provider at all locations.
   b. Co-ordination, troubleshooting and resolution of reachability issues for third party networks terminated at respective locations.
   c. Co-ordination, troubleshooting and resolution reachability/access problems to servers, databases, devices etc., along with respective teams for smooth access to applications hosted at DC and DR by the bank's users.
   d. Call logging and coordinating with vendor in case of failure of network hardware, third party connectivity, HPE IMC software etc.
   e. Co-ordination with CSOC service provider during switch port security issues, log shipment, access related issues, troubleshooting and resolution.
   f. Co-ordination with FM for application access related issues.
   g. Co-ordination with LAN cabling vendor for cabling related issues at DC, DR and branches. The cabling vendor will be contracted by the bank.

3. **Configuration Management**

   a. Installation/Configuration/integration of network switches, including those that would be added by the bank during period of contract.
   b. VLAN Management - Add/Move/Change/Delete VLANs at DC, DR and branches (currently L3 switches are deployed at four locations only). The bidder to note that based on bank's requirements L3 switches may be extended to other locations also during period of contract.

c. ACL Management – Add/Delete/Change ACLs on network switches at DC, DR & branches based on requirements for hosting of various applications & services, third party vendors, security & monitoring solutions, architectural changes etc.

d. Switch Port security configuration and management on all access switches across the organisation.

e. Changing configuration on aggregation switches, based on the bank requirements for termination of WAN links, third party links/services etc.

4. **Segmentation** - Design/Create/manage/disable network segmentation based on banks requirement and Industry best practices for installation of servers, databases, security devices and other solutions in various segments. This task to be carried out in coordination with ISA.

5. **Security Management for network**

   a. Defining & Maintaining baseline security requirements/configurations and documenting for all the categories of network devices (switches, routers etc.), operating systems etc. The documents are to be updated periodically and submitted to the bank for review.

   b. Ensuring secure configuration and documentation of all access points, nodes between (i) different VLANs (ii) LAN/ WAN interfaces (iii) bank's network to external network and interconnections with partner, vendor and service provider networks.

   c. Disabling unused interfaces and unwanted network services.

   d. Review of routing protocols, if any, configured on LAN.

6. **Inventory & Architecture Management**

   a. Maintaining up-to date inventory of all the network assets (switches, third party routers and other network devices). The inventory should include all the interfaces, IP address, IOS version, configuration, open & closed ports, VLANs, ACLs etc.

   b. Maintaining up-to-date network architecture diagram, both low and high level at DC, DR & branches and periodic updation. For branch LAN coordination with Facility Management team.

   c. Maintenance of AMC/Warranty details of all LAN devices and intimation to the bank as and when AMC/Warranty is due for renewals.

7. **IP Schema Management**

   Maintaining, Allocation, Deallocation and periodic updation & review of IP schema across the organisation, including IPs provided by third party vendors/service providers for different services and public IPs procured from Internet service providers.

8. **Upgradation & Patching**

   a. Upgrade of IOS on switches / routers (Banks own), HPE IMC software as and when released by the OEM. In case of third party routers & CPE co-ordination with service provider for upgradation.

   b. Applying patches to all the network devices as and when released by OEM. The engineer to periodically visit the OEMs website for checking the availability of patches. Patch management will be manual and in case bank procures any tool, the patch management to carried out through the same.

9. **Implementation & Integration**
   a. Implementation of network hardware in coordination with vendor, as per requirement of the bank .
   b. Integration of all network devices (other than SDWAN) with SIEM for log collection, analysis and co-relation, PIM (secure access to administrators) and other applicable solutions, if any, provided by the bank during period of contract, for which assistance of the vendor would be provided.
   c. Integration of all network devices, including branch switches, with HPE IMC software tool for monitoring, alerting etc.

10. **Link Load balancers**
   a. Configuration, Re-installation, Management, Monitoring, Hardening, Upgradation (including patches and software as and when released by OEM) of link load balancers at DC and DR.
   b. Creation & Management of sub-domains on link load balancers.
   c. Co-ordination with ISP / third party for maintenance (add/delete/change/shift) of DNS records.
   d. Setting up of QoS on link load balancers based on Bank requirement.
   e. Continuous Monitoring and troubleshooting.

11. **Internet**
   a. Monitoring of Internet links and co-ordination with ISP for restoration of failed link(s).
   b. Periodic monitoring of internet links for bandwidth utilization and updating the bank in case of requirements for upgrade.
   c. Implementation of Internet links in coordination with ISP as and when procured by the Bank.
   d. Co-ordinating with Internet service provider for carrying out configuration changes, hardening, patching etc.
   e. Coordination with service providers for hardening of routers. The hardening of routers will be carried-out by the vendor providing network / internet links. However, bidder will be required to guide / help the bank in defining hardening specifications and will also coordinate with service provider for implementation.
   f. DDOS management
   Bank has subscribed to DDOS protection from respective Internet service providers. The subscription is for protection against volumetric attacks.
   The network engineer has to review the attack details submitted by the service provider and intimation for mitigation.

12. **Web Gateway Security (WGS)**
   a. Installation / re-installation / configuration / Hardening / management of Web Gateway Security (Proxy) appliance. Need based Support of OEM / 3rd party vendor to be taken during installation/configuration.
   b. Blocking / Un-blocking of - websites, Internet downloads, ports, content filtering etc., as per operational requirement.
   c. Creation / maintenance / documentation of policies on WGS as per SIDBI

guidelines.

d. Periodic review of policies on WGS.

e. Monitoring of signature updates, disk space, CPU utilization, Memory utilization etc., of appliance. Also includes updation of signatures in the appliances.

f. Configuration of WGS for forwarding the logs to log monitoring/collection tools.

g. Uploading of configuration to secondary appliance as and when changes are carried out on primary appliance.

h. Periodic / critical reporting to SIDBI officials based on WGS activities / logs.

i. Generation of reports on daily basis for determining usage pattern i.e., top users, top websites visited, malwares detected etc. and reporting to Bank.

13. Others

a. Backup of configuration files as per backup policy of Bank and during any configuration changes etc.

b. Labeling of all the cables, MUX, Patch Panels etc., at DC and DR.

c. Re-arranging of network equipment in the same / different rack at DC and DR.

d. Co-ordination with vendor / OEM / Service provider during RMA.

e. Maintaining & Updating of SOP, hardening & baseline documents etc.

f. Providing timely compliance to various - audit observations (internal/external), VAPT, Advisories from regulators, ISO audits etc., for bank owned devices. In case of equipment (third party networks) coordinating with Service provider for providing compliance.

g. SLA Management with vendors.

h. Update/ Maintain Standard Operating Procedure (SOP) documents.

14. Reporting

Maintenance of daily / Weekly and monthly uptime/downtime report of LAN devices, Link load balancers etc.

SIDBI's Responsibilities

a. To provide requisite Software, licenses and OEM/ Support vendor / Service providers/Escalation details.

b. To provide contact details of branches and vendors.

c. To provide necessary approval to the Change requests.

d. To provide policy, SOP, hardening/baseline documents etc., if any.

e. To provide existing architecture diagrams, IP Schema, VLAN details, Public IP details.

6.4.19 Patch Management Services

SIDBI has currently deployed Microsoft **Windows Server Update Services** (**WSUS**) for patch deployment on Wintel Servers using hub-and-spoke model. Patches on Linux/ UNIX Servers and other devices like security devices, Web secure gateway, Network devices, Citrix NetScaler etc. are done manually. Patch management is done centrally from Datacenter.

During the contract period, if Bank decides to use any other tool for patch management, Service Provider shall use the same.

Service Provider's Responsibilities

1. Install and test patches and updates in Test environment. Test environment to be provided by SIDBI. Wherever, test environment is not available, the patches need to be applied first in Development / UAT / DR environment and thereafter at production environment after approval from SIDBI.
2. Install / implement security releases / patches based on advisories received from Government agencies viz. DIT, IDRBT, NCIIPC, RBI etc.
3. Roll back if acceptance fails.
4. Take necessary approval from SIDBI for shutdown or re-start, if required, for patch or update implementation.
5. Raise Change Management for deployment of patches or updates both in UAT and production environments.
6. Schedule shutdown of production system and inform users.
7. Implement patches as per approved deployment strategy.
8. Follow up and co-ordinate with OEM/ 3rd party support vendors for patch deployment on non-wintel devices.
9. Root Cause Analysis (RCA) for Security incidents.
10. Providing timely compliance to the audit observations related to patch management as observed during various internal/ external audits.
11. Prepare and maintain Standard Operating Procedure (SOP) document pertaining to the service.

SIDBI's Responsibilities

1. To provide requisite Software, licenses and OEM/ Support vendor details.
2. To provide necessary approval to the Change requests.
3. To provide policy and SOP documents, if any.

6.4.20 EMS Tools Management

As mentioned in above sections, SIDBI is using HP Open View suite of EMS tools for the effective management of its IT Infrastructure. The Service Provider would continue to make use of these tools for the Help Desk and management of other services as mentioned in the RfP. An indicative list of responsibilities but not limited to, is given below. The SP is required to manage/ configure/ use these EMS tools to provide services as per scope of RfP.

Service Provider's Responsibilities

1. Install, re-install and configure respective tools as per bank's requirements prescribed in this Rfp and any other requirement that arises during the course of the contract.
2. Upgrade / Updation / Implementation of any new version or patch released by the OEM vendor.

3. Service provider to ensure continuous efforts for innovative use of the EMS tools to ensure optimum effective utilization of these tools towards achieving business goals of the bank and thus justifying the ROI.
4. End-to-end management of the tools with respect to configuration, hardware, database or any other performance issues.
5. Configuration of any new device, service or office location added to the Infrastructure.
6. Maintenance of the underlying databases, application servers, OS or any other software
7. Maintenance of the Configuration and Management Database (CMDB).
8. Suggest SIDBI from time to time on the sizing requirements of the Servers, Databases and licenses so as to avoid performance issues, if any. However, SP will address the issue itself wherever same is under the scope of the project.
9. Customization of End-user interface and reports on an ongoing basis as per bank's requirements.
10. Service Provider needs to keep at least one resource on-site with requisite skill and experience to manage all the EMS tools after implementation on continuous basis. He must be involved from day-1 with all implementation activities and SP must arrange for suitable training for him as and when required.
11. In case of on-site team not being able to resolve any issue, Service provider shall take help from their back-end team or from OEM so as to resolve the issue within prescribed SLA.
12. Any other integration with either HP EMS tool components or SIDBI's other applications, if technically feasible, for better productivity.
13. Providing timely compliance to the audit observations related to EMS Tools infrastructure as observed during various internal/ external audits.

SIDBI's Responsibilities

1. To provide requisite Software, licenses and OEM/ Support vendor details.
2. To provide necessary approval to the Change requests.
3. To procure additional licenses, if required.
4. To renew software support (ATS) for respective tools/ databases with OEM wherever it is not under the scope of the Service Provider.
5. To upgrade the underlying hardware as per Service Provider's recommendations, wherever it is not under the scope of the Service Provider.
6. To provide policy and SOP documents, if any.

6.4.21 Disaster Recovery (DR) Site Management services

1. Currently SIDBI has its DR Site co-located at 3rd part Datacenter at Chennai with necessary infrastructure in place to support Bank's DR Policy (DRP). DR Policy is subject to periodic reviews and updates leading to infrastructure changes and updates.
2. Application servers are synchronized with DC Servers by applying the application releases / patches/ updates.
3. Databases are synchronized by sending and applying the archive logs using Oracle Data-guard (Hot Standby).

4. Periodic BCP testing / DR Live operations are conducted (presently half yearly) to re-assess the effectiveness of the DR site. DR Live operation involves the users from all offices carrying out their normal business operations from DR site for a specific period decided by SIDBI.
5. In the event of any disaster or for DR Live operations, Activation and de-activation of DR Site is the joint responsibility of DC and DR Teams. Both the teams are required to perform their roles and duties as prescribed in the DRP and other guidelines given by SIDBI from time to time.

Service Provider's Responsibilities

1. Normal Operations

a. Performing all the activities as mentioned under **Section 4.4. Statement of Work for DC operations** will also be required to be performed for DR Site.
b. Ensuring synchronization of database of DR site with that of production database at DC.
c. Ensuring backup and restoration of Application and Database servers as per the bank's backup policy.
d. Arranging for the compliance to the observations made during IT and other internal audits of the DR Site. Service provider shall suggest and recommend infrastructural requirement, if any to SIDBI for the purpose of giving audit compliance.
e. Provide support for BCP testing and DR live operation.

2. Disaster Management

In case of disaster at Datacenter, following activities need to be performed at the DR Site till the primary Datacenter is recovered and operational.

a. Coordination with the DR Team for the activation/ de-activation of the DR Site.
b. Coordination with the FM Support teams/ ITV Nodal Officers at respective locations and Application support teams to ensure that the users are able to access and perform operations from DR Site.
c. Database Administration of DR Site databases. (Including activation of database at DR Site for operations).
d. Citrix Farm, VMWare and Active Directory administration.
e. Backup and storage management
f. Middleware application tools administration.
g. E-Mail Management
h. Network Management and Security Monitoring.
i. If required, Service provider may be required to deploy additional resources at DR Site to provide necessary support till the restoration of primary site. Additional resource may be taken from the resource pool at primary site.

SIDBI's Responsibilities

1. To provide requisite Software, licenses and OEM/ Support vendor details pertaining to DR Site.
2. To provide new/ upgrade the existing hardware to meet DR requirements of SIDBI from time to time.

3. Provide DR Policy, DR Site activation/ De-activation and other necessary guideline documents.

6.4.22 Annual Maintenance Contract (AMC) Services

1. AMC Services for various items at all respective SIDBI locations are required with effect from November 01, 2021. Office wise details of the items along with the effective date of start of AMC are given in **Appendix-VIII**. Accordingly, while providing for the quarterly cost breakup of the services, AMC charges calculation would be done on pro-rata basis starting from the said date.
2. Any equipment coming out of warranty/ AMC currently with third party shall automatically come under AMC with the Service Provider. Therefore, all such items must be taken into consideration for AMC calculation for the remaining period of the contract.
3. Service provider will be required to provide AMC for hardware items either **directly or through the respective OEM vendor**.
4. At any stage of the contract, SIDBI reserves the right to terminate the AMC for any of the item(s), with due prior notice to the service provider. Payment made in advance towards the AMC charges of the items being taken out of AMC shall be adjusted from the payment for the following quarter. Service provider shall raise invoices for subsequent quarters after deducting the AMC charges for the items taken out of AMC.
5. AMC for the items listed in **Appendix-VIII** is required from '**AMC From Date**' to '**AMC To Date**'. In case bank desires to have the AMC of these items beyond the '**AMC To Date'**, the Service provider shall continue to provide the AMC services till the replacement of these items at the AMC rate applicable for the last quarter or average AMC rate applicable for last 4 quarters, whichever is less. However, Bank shall issue separate purchase order for continuance of AMC Services of the items beyond '**AMC To Date',** if so desired by the Bank.
6. If SIDBI acquires new IT asset(s) after the start of this contract and after the expiry of essential warranty period bank decides to go for the AMC of these items with service provider, AMC rate for such items will be determined based on the unit AMC rate already decided for the similar other item.

Service Provider's Responsibilities

1. The type of maintenance will be fully comprehensive on-site including repair / replacement of parts or full item, in case the same not repairable, with same or better configuration / technical specifications. Maintenance Services shall consist of preventive and breakdown maintenance of the items covered under AMC at respective locations.
2. All maintenance services including patching / firmware upgrade / signature updation etc. is required to be attended by SP.
3. Fault identification and trouble shooting.
4. Identify spares requirement for problem resolution
5. Make sure that calls are attended and resolved as per agreed SLAs.
6. Plan for standby equipment to be available at strategic locations to ensure that hardware downtime is minimal.
7. Maintain requisite level of inventory of spares for the hardware items especially the servers under AMC at strategic locations.

8. Proper recording of calls details, response and resolution details with sign-off (manual or electronic).
9. Reports for downtime, problem resolution and response details should be available to SIDBI.

<u>SIDBI's Responsibilities</u>

1. Allow access to vendor's maintenance personnel or Service Provider of the hardware under AMC/ warranty at respective SIDBI locations for the purposes of problem diagnosis and repair;
2. Provide hardware upgrades and replacements (which is not provided under warranty or maintenance agreement);
3. Provide contract details of all the 3rd party warranty/ AMC service providers.

6.5 Statement of Work – Application Services

To support its business and administrative functions, SIDBI has implemented/ deployed a wide stack of business applications, support applications, business-efficiency enhancement tools, security components etc. Applications vary from standard and/or customized 3rd party software products as well as in-house developed legacy applications developed on technology platforms like Oracle Forms 12c, JAVA, .NET etc.

End-user support for all these applications is provided by the resources of the existing service provider. Underlying technology tools also require regular maintenance, administration, tuning for improvement of performance etc.

6.5.1 Application Support Services

Presently, support services are required for the following applications. However, support will also be required to be provided by the service provider for any other application added during the contract period.

List of Applications – Support Required

S.N.	Application Name	Use of the Application
1	SSO	Single Sign-on linked applications accessed over Intranet. (Citrix based & Web based)
2	Application Logon 12C	To access Legacy Applications
3	Management Information System (MIS)	MIS and Exposure monitoring system,MIS Dashboard
4	Customer Management	Customer complaint management software
5	Flexcube GL / CIF – Oracle	Flexcube GL / CIF – Oracle
6	Flexcube Interface, GL Reports	Flexcube Interface and GL Reporting
7	Direct Finance System (DFS)	Term loan management and accounting including Working Capital, bank Guarantee schemes and Non-treasury Investments.
8	Receivable Finance Systems (RFS)	Bill / Invoice discounting management and accounting.
9	Recovery and NPA Management System (RNMS)	Management of NPA accounts, Security management
10	Resource Management System (RMS)	Term deposits and priority sector deposits.

List of Applications – Support Required		
S.N.	**Application Name**	**Use of the Application**
11	Smart Application/Report	Credit appraisal and rating system
12	Online Loan Application	Online Loan Application
13	Nominee Director	Nominee director
14	General Payment Processing System (GPPS)	Front-end voucher entry and inter-branch accounting, vendor payments
15	Payment and Collection System (PnC)	Payments, collection management and daily fund management
16	HRMS	Software for HR Management
17	Visitor Management System (VMS)	Issuing gate pass for Lucknow head office
18	Hindi Vertical	Report for Hindi statistics
19	Payroll System (CSPC & ADMPAY)	Salary processing software
20	Common Administrative Payments (CAP)	Staff administrative payments / Reimbursements/ Loans & Advances.
21	Terminal Benefit System (TBS)	Managing terminal benefits like PF, Pension and Gratuity
22	RTI System	Monitoring of RTI applications
23	DFMS Software	Document & File Management System (DFMS) will improve the operational efficiency of Bank by capturing & tracking End-To-End movement (Inwarding & Outwarding)
24	Vigilance Application	Reporting module for vigilance application
25	Litigation Management	Monitoring of legal case against sidbi bank
26	Audit Software	Procedures pertaining to various activities of the Bank.
27	Due Diligence software	Managing IBA third party entity & IBA fraud list, Caution Advice & Wilful defaulter list, CIBIL, Machinery Supplier Database System
28	Fixed Asset Software / Centralized Depreciation System (CDS)	Dead stock management software
29	Fixed Deposit Application - Customer Facing application	Fixed Deposit Application - Customer Facing application
30	Retired Employee - portal	Benefit system for retirees
31	SIDBI KYC (NSDL)	Verifying the identity of customers
32	P&D	Promotion & Development
33	Udyami Mitra Portal	Udyami Mitra Portal Application

A description of the envisaged scope under this category is enumerated as under.

1. DC/ DR team will ensure deploying patches for Applications (In-house / products) as advised by SIDBI team, both at DC and DR.
2. Tracking, Responding & Resolution of all the Support Request submitted by end-users of the applications rolled out in production environment.
3. Maintenance of all Support Request in 'Service Manger' Central Help Desk or any other tool as decided by SIDBI.

4. Providing telephonic Support to users of all SIDBI branches for all the applications.
5. Handholding / Educating users by shadowing user session for all the applications.
6. Ensuring resolution of Support Request as per the timelines/ SLA specified.
7. Meeting user requirements by providing data in structured format using queries provided by SIDBI Team(s).
8. Based on the nature of support request, service provider will be required to define SQL queries for resolution of data related issues and take approval from concerned SIDBI Team before execution.
9. Coordinate and follow-up for resolution of all the Support Request with respective SIDBI – ITV Team, if required.
10. Monitoring, Coordination & Resolution of User Support / Day-end related issues with concerned DC/ DR/ Application Team.
11. Update knowledgebase based on experience of closure of each call.
12. Performing Root cause Analysis – Functional.
13. Coordination and follow-up with other support groups, as required.
14. Adherence of SLA for all the applications related issues.
15. Coordination with Level-3 support (respective application vendors or SIDBI's internal component owners) for resolution of all the calls.
16. Logging and tracking the calls with OEMs for support related to respective products, viz. 'Global Support Desk' of Oracle for Flex-cube related problems etc., in discussion with SIDBI ITV team.
17. Assisting the Bank's team in terms of software audit and audit compliance for all these applications.
18. Creating repository for Issue logs, FAQs and other such artifacts for each of the applications.
19. Submission of issue logs / summary of approved changes undertaken in support activities.
20. Maintain & submit report(s) for various application patches deployed on periodic basis as advised by SIDBI.
21. Vendor to ensure End-of-Day (EOD) of Flexcube in co-ordination with various users, through e-mail, messaging and telephone contacts.
22. Periodic Closing of Accounts Support in association with SIDBI / concerned 3rd party vendor / team, beyond prescribed service window.

6.6 Miscellaneous Activities

6.6.1 Documentation and Reporting

Service provider shall be required to provide at least following documents at different phases during the contract period. If need be, service provider shall also update the existing documents like process documents, system/ user manuals etc. This is an indicative but not exhaustive list of documents. Actual requirement will be spelt out during signing of contract or during the lifecycle of the project. Additional documents may also be required to be provided based on requirements during the lifecycle of the project.

6.6.1.1 Documentation

1. Process documentation – updating the documents for current processes and preparation for the newly introduced processes during the contract period.

2. Service provider should maintain/ prepare/ update below mentioned documents for each of the area of the DC & DR operations i.e. Wintel, Linux/ Unix, DBA, Middleware, EMS Tools, Network, Citrix, VMWare, Backup & Storage, Office365, Messaging (Exchange/ IBM Notes), Application Support, Network, Information Security etc.

   - Standard Operating Procedures (SOPs)
   - Technical Architecture Manual (TAM)
   - Technical Operational Manual (TOM)
   - Low level and high-level Network diagrams for DC & DR.
   - Detailed architecture document for the applications deployed/ to be deployed in DC/ DR. These documents shall contain details of all the interface/ integration points/ port details with other applications/ servers/ databases/ network & security devices/ port details etc.

3. User requirements Document for newly introduced processes, if any. Existing documents shall have to be updated in case of requirements change.

6.6.1.2 Reports

Vendor shall configure & submit the reports on a regular basis in a mutually decided format. The following is only an indicative list of reports. Based on the requirement service provider will be required to configure & provide additional reports. Softcopy of these reports shall be delivered automatically via email / Dashboard at specific frequency and to the pre-decided list of recipients. Role based selection of reports, selection of name of the recipients of the reports, frequency of delivery must be parameterized /configurable in the EMS tool.

SP shall submit certain information as part of periodic review as and when required by the Bank. Service provider will provide all the required reports wherever not getting generated from EMS tool.

Following is the indicative list of reports:

1. **Daily reports (to be submitted on next working day)**
   - ❖ Summary of issues / complaints logged at the Help Desk.
   - ❖ Summary of resolved, unresolved and escalated issues / complaints.
   - ❖ Summary of resolved, unresolved and escalated issues / complaints to OEMs/ vendors/ SIDBI support teams.
   - ❖ Log of backup and restoration undertaken.
   - ❖ Server / Database Utilization Report.
2. **Weekly Reports (to be submitted on the first working day of the following week)**
   - ❖ Issues / Complaints Analysis report for virus calls, call trend, call history etc.

- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.
- Summary of changes undertaken in the DC and DR including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

3. **Monthly reports (to be submitted by 10th of the following month)**
    - Component wise physical as well as IT infrastructure availability and resource utilization
    - Summary of component wise DC and DR uptime.
    - Summary of changes in the DC and DR.
    - Log of preventive / scheduled maintenance undertaken
    - Log of break-fix maintenance undertaken
    - Configuration Management summary report.
    - Change Management summary report.
    - Release Management summary report.
    - Capacity Management summary report of servers.
    - Service Level Management – priority/ severity wise response and resolution.
    - Service Failure Analysis, listing out escalations and downtime/ outages, if any.
    - Account Dashboard, listing out:
        - Planned activities carried out during the month.
        - Unplanned activities carried out during the month.
        - Activities planned but missed along with reasons.
        - Challenges faced during the month.
    - Service Operations, listing out:
        - Helpdesk Management, listing out priority/ severity wise calls logged with comparison for past three months.
        - Incident reporting & Management, giving category wise call details for critical service areas with comparison for past three months.
        - Operational Activities
        - Location wise attendance of the on-site resource personnel.
        - Service wise performance of activities as per scope of individual service areas.
    - Service Improvement Plan, listing out:
        - Concerns/ Escalations with action plan.
        - Planned activities/ initiatives.
        - Improvements planned, if any.
4. **Incident Reporting (to be submitted within 48 hours of the incident)**
    - Following incidents, but not limited to, should be reported within 48 hours to Incident Reporting (IR) Desk of CISO Team:
        - Environmental controls, Physical security violations/ threats at DC and DR.

- Hardware breakdowns leading to services interruptions.
- Software license violations.

6.7 Service Window

Following is the service window to be followed by the Service Provider.

Service Area	Service Window	Time Period * Shift – I	Time Period * Shift – II
Program Management & Operations Management	9 hrs x 5 days	09:30 AM– 06:30 PM	
Data centre / DR site services / Middleware tools management/ E-Mail	12 hrs x 5 days	08:30 AM – 04:30 PM	12:30 PM – 08:30 PM
	Week-end / National Holiday	* Needs based Skeleton support (Maintenance activity etc.)	
Application Support & Overall Help Desk	11 hrs x 5 days	09:00 AM – 05:00 PM	12:00 PM – 08:00 PM
	Week-end / National Holiday	Need based Support (Minimum 1 Resource)	
EOD Support	8 hrs x 6 days	02:00 PM – 10:00 PM	

*** Time period is indicative and is subject to change. Staggered duty may be considered beyond normal office hours.**

6.8 Staffing requirements

Bidders / Service provider may kindly note that the quality of staff deployed to manage the contracted services is of utmost importance to the Bank. It is needless to mention that bank will reserve the right not to accept any of the staff members deployed, if he/ she is not found up to the mark as per bank's expectations/ requirements. Vendor will be responsible for any delay in delivery on account of such non-acceptance of staff by SIDBI consequent upon deployment of inappropriate staff/personnel.

Following points may be noted by the bidder in connection with plan of staffing in this project:

6.8.1 Skill-set / Qualification / Experience

- ❖ Minimum desired educational qualifications and the experience/ skill-set possessed by resources is given below.
- ❖ The bidder to ensure that deployed resources should work as a team & interact in cohesive environment to resolve potential conflicts and implement positive changes.

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
Infrastructure Support Services			
1	Program Manager	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M.Sc. (IT) / M.Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory**: Certification of ITIL Foundation or above	○ Should have handled similar DC/DR - fIT Infrastructure management projects in an Enterprise environment. ○ 10+ years on ITIL framework-based project management. ○ Experience of managing IT infrastructure using ITIL tools. ○ Should have strong written, verbal and presentation skills ○ Must be on the rolls of the service provider since at least of 01 year prior to posting at SIDBI.
2	ORACLE Database Administrator (DBA)	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory:** Oracle Certified Professional (OCP-DBA 12c or above) certification is a must.	○ Should have worked as core Database Administrator (DBA) in an Enterprise environment. ○ Should have worked on Oracle 19c and above deployed in Windows, Linux and Unix platforms. ○ Should have good knowledge of Diagnostic & Tuning pack, RMAN, RAC, Dataguard, and HP UNIX .
3	Unix & Linux administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory:** Certification in UNIX administration, preferably HP-UNIX or Linux.	○ Should be working as a core UNIX (HP UNIX, Linux) Administrator in an Enterprise environment. ○ Should have good understanding of storage environments (SAN, NAS etc.), System backup, installation & configuration, tuning, HP –UNIX / Linux shell scripting and networking.
Wintel Group: Deployed resource should have mix of skill set in following areas: ○ Server (Wintel) Administration, ○ Antivirus and Patch Management ○ Citrix Administration, ○ VMWare Administration			

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
4	Server (Wintel) Administration	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory**: MCSA – Windows Server (Microsoft Certified Solutions Associate (MCSA) Certification.	○ Should be working as a core Wintel Server Administrator in an Enterprise environment. ○ Should be able to handle Servers Management including **Active Directory** ○ Should be able to configure and install Intel servers, maintain the Change Management Process for any change in server configurations, perform regular antivirus monitoring, patch management and Enterprise backup management using automated solution. ○ Should be well versed with Server Virtualization, DHCP, DNS, WINS, SMTP, POP3, RAS and VPN, etc. ○ Should be able to install, configure and manage Antivirus Servers (Symantec)
		○ Graduate in Computer Science / IT / Computer Applications (BCA) from a recognized university. ○ **Mandatory**: MCSA – Windows Server (Microsoft Certified Solutions Associate (MCSA) Certification.	○ Should be working as a core Wintel Server Administrator in an Enterprise environment. ○ Should be able to handle Servers Management including **Active Directory** ○ Should be able to configure and install Intel servers, maintain the Change Management Process for any change in server configurations, perform regular antivirus monitoring, patch management and Enterprise backup management using automated solution. ○ Should be well versed with Server Virtualization, DHCP, DNS, WINS, SMTP, POP3, RAS and VPN, etc. ○ Should be able to install, configure and manage Antivirus Servers (Symantec) ○ Should have minimum 03 years of experience in addition to experience defined in Section 6.8.2

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
5	Citrix Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory**: Citrix Certified Administrator (CCA) for Citrix XenApp 4.0 or above.	○ Should be working as a core CITRIX Administrator in an Enterprise environment. ○ Should have good working knowledge of installing, configuring and managing a Citrix Server Farm with 20+ servers and 300+ user licenses. ○ Experience on essential Citrix components like Web Interface, License server, Citrix Netscalar, Secure Ticketing Authority, Citrix XenServer Enterprise edition
		○ Graduate in Computer Science / IT / Computer Applications (BCA) from a recognized university. ○ **Mandatory**: Citrix Certified Administrator (CCA) for Citrix XenApp 4.0 or above.	○ Should be working as a core CITRIX Administrator in an Enterprise environment. ○ Should have good working knowledge of installing, configuring and managing a Citrix Server Farm with 20+ servers and 300+ user licenses. ○ Experience on essential Citrix components like Web Interface, License server, Citrix Netscalar, Secure Ticketing Authority, Citrix XenServer Enterprise edition ○ Should have minimum 03 years of experience in addition to experience defined in Section 6.8.2
6	VMWare Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory**: VMWare Certified Professional (VCP).	○ Should be working as a VMWare Administrator in an Enterprise environment. ○ Should have hands-on experience and proficiency in managing and maintaining a medium/large environment (100+ Servers) ○ Should be able to handle Servers Management including **Active Directory**

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
7	Backup-Recovery & SAN Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory:** Certified Symantec Netback Administrator for NetBackup 5.0 or above OR Certified SAN Administrator.	○ Should be working as a System Administrator handling SAN Storage Management, Backup-recovery management in an Enterprise environment. ○ Should be able to manage backup and recovery process as defined by the bank, define and modify backup policies, tape movement to/ from off-site backup locations, co-ordinate with remote offices to ensure backup and recovery as per policies.
08	Network Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory :** For L1 – CCNA For L2 – CCNP (Routing and switching OR Enterprise)	○ Should be working as a core Network Administrator in an Enterprise environment. ○ Should have worked on routing and switching , VPN, VLAN etc. ○ Good understanding of Network Architecture & Protocols, VLAN, dynamic routing protocols, VPN, IPsec, load balancers, DNS etc.
09	Security Manager	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory:** CISM/CISSP	○ Should be working as a core security Administrator in an Enterprise environment. ○ Good understanding in designing Security Architecture, designing security policies / guidelines / process, encryption, Log analysis etc
10	Firewall Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory:** NSE4 (Fortinet) /CCSE (Checkpoint)/ PCNSA (Paloalto) /SNSA (Sonicwall)/ CCNP Security/ or similar certification in other OEM firewall	○ Should have worked as a NGFW & NIPS administrator. ○ Good understanding in installation, configuring, managing and monitoring of NGFW. ○ Should have worked on configuration and management of site-to-site, client-to-site VPN.

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
11	Mail Administrator	**Office-365 Portal Administrator** ○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ **Mandatory**: Microsoft 365 Certified Associate.	○ Should be working as a core Office-365 portal Administrator. ○ Should be proficient in Exchange Administration, ADFS, Federation Services and SSO, Domain Name Services, Microsoft Azure, SharePoint Administration, PowerShell etc. ○ Should have strong understanding of day-to-day functionality in Microsoft services like Teams, Skype, One Drive, Exchange, and Active Directory.
		Office-365 Portal Administrator ○ Graduate in Computer Science / IT / Computer Applications (BCA) from a recognized university. ○ **Mandatory**: Microsoft 365 Certified Associate.	○ Should be working as a core Office-365 portal Administrator. ○ Should be proficient in Exchange Administration, ADFS, Federation Services and SSO, Domain Name Services, Microsoft Azure, SharePoint Administration, PowerShell etc. ○ Should have strong understanding of day-to-day functionality in Microsoft services like Teams, Skype, One Drive, Exchange, and Active Directory. ○ Should have minimum 03 years of experience in addition to experience defined in Section 6.8.2
		IBM -Domino Administrator ○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute.	○ Should be working as a core IBM Domino Administrator on Domino 9 or higher in an Enterprise environment. ○ Should be able to install, configure and manage Domino servers, manage notes & non-notes clients, clustering of domino servers, write/ configure mail routing rules as per business rules, database replication across domino servers.

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
		<u>IBM -Domino Administrator</u> ○ Graduate in Computer Science / IT / Computer Applications (BCA) from a recognized university.	○ Should be working as a core IBM Domino Administrator on Domino 9 or higher in an Enterprise environment. ○ Should be able to install, configure and manage Domino servers, manage notes & non-notes clients, clustering of domino servers, write/ configure mail routing rules as per business rules, database replication across domino servers. ○ Should have minimum 03 years of experience in addition to experience defined in Section 6.8.2
<u>Middleware Group</u>: Deployed resource should have mix of skill set in following areas: ○ Middleware Application Management ○ EMS tools Administration			
12	Middleware Application Management	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute.	○ Should have experience in Installation, Configuration, Administration, troubleshooting etc. on middleware software tools as mentioned at **Section 6.4.10** : Middleware – Application Management Services. ○ Administrator for "Oracle Forms and Report Server (Oracle WebLogic)" and "IBM WAS & IBM MQ" should have <u>minimum 03 years of relevant experience</u>.
13	EMS tools Administrator	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute.	○ Should be working as EMS tools Administrator in an Enterprise environment. ○ Should have experience of at least one enterprise level of implementation / management of Microfocus (HP)-EMS tools (SM, OM, NNM) currently being used by SIDBI.
Application Support Services			
14	Application Support / EOD Support	○ Engineering Graduate in Computer Science / IT / ECE or MCA / M. Sc. (IT) / M. Sc. (Computer Science) from recognized University / Institute. ○ Good domain knowledge in banking	○ Should have experience of providing User Support on banking applications including core banking applications. ○ Should have experience of SQL.

Srl. No.	Resource Details	Minimum Educational Qualifications	Skill Set
		○ Graduate in Computer Science / IT / Computer Applications (BCA) from a recognized university. ○ Good domain knowledge in banking	○ Should have experience of providing User Support on banking applications including core banking applications. ○ Support Team member(s) deployed for extending User Support **<u>should have minimum 03 years of experience in addition to experience defined in Section 6.8.2</u>** ○ Should have experience of SQL.
15	Help Desk	○ Graduate in any discipline from a recognized university. ○ Good domain knowledge in handling IT Help Desk using any Help Desk Software preferably in banking domain.	○ Support Team member(s) deployed for extending Help Desk Support should have minimum 03 years of experience for providing user support on banking applications including core banking applications.

6.8.2 Experience Level

Experience level of the staff members may be referred as follows:

Level of Experience	Total Minimum Experience	Minimum relevant Experience in the Core Domain Area
L1	3 Years	2 Years
L2	5 Years	3 Years
L3	8 Years	5 Years
Program Manager (L3^{+})	15+ year	10 Years

6.8.3 Minimum requirement of on-site Resources

Service provider shall deploy minimum number of on-site resource personnel as indicated below at Mumbai, Chennai and Lucknow Offices. However, with a view to achieve desired SLAs for respective services, bidders may plan and propose additional resources at various service verticals.

The Service Provider must look for right mix of experienced skill-set to optimize the number of resources and thereby help SIDBI in controlling overhead expenditure on account of infrastructure and similar other factors.

S. N.	Service Area / Domain	Resource Location	Minimum number of on-site resources Required			
			Experience Level wise proposed no. of resources			Total No. of resources
			L1	L2	L3	
			a	b	c	d= a+b+c
1	**Program Manager**	Mumbai	-	-	1	1 [L3^{+}]
2	**Data Base Administrator**	Mumbai	-	2	-	2
		Chennai	-	-	-	
3	**Unix Administrator**	Mumbai	-	1	-	3
		Chennai	1	1	-	
4	**Network Management**	Mumbai	1	1	-	3
		Chennai	-	1	-	
5	**Firewall Administration**	Mumbai	-	1	-	2
		Chennai	-	1	-	
6	**Security Administration**	Mumbai	-	-	-	1
		Chennai	-	-	1	
7	**WinTel - Server Administration (WinTel, Antivirus, Patch Management), CITRIX & VMWare Administrator**	Mumbai	1	2	-	5
		Chennai	1	1	-	
8	**SAN Storage & Backup Management**	Mumbai	-	1	-	1
9	**Mail / O365 Administration**	Mumbai	1	1	-	2
		Chennai	-	-	-	
10	**Middleware Application Management + EMS Tools Mgmt**	Mumbai	2	2	1	7
		Chennai	1	1	-	
11	**Application Support Mgmt + EoD**	Lucknow	5	3	-	8
12	**Help Desk - All India**	Lucknow	2	-	-	2
Total No. of Resources			**15**	**19**	**3**	**37**

- Bidders may make its own assessment on the level and number of resources beyond minimum level as per its service delivery management.
- For manpower consideration all the employee should be on the payroll of the Bidding Company.

The Bidder may please note the following in connection with resource deployment.

- The shortlisted Bidder will have to introduce the resources (throughout the period of contract) to Bank via formal communication on company letterhead along with copies of qualification, experience, certifications and biodata. On receipt of the information, the bank would conduct interview of the resources before finalizing. The bidder has to deploy the resource based on the confirmation from the bank.
- The shortlisted Bidder shall deploy ALL resources, who should be in their **OWN PAYROLL**. Undertaking from company along with latest payslip to be submitted.
- It will be the Bidders responsibility to get their identity & address proofs submit to the Bank. The shortlisted bidder has to carry out following checks for all resources deployed on the site during period of contract:
    - Background verification - including education and experience of all the resources deployed on-site and submit the certificate.

  - Police verification (PV) - of all the resources deployed onsite at the bank and submit certificate.

- The background and Police verification certificates to be submitted within 3 months from the date of joining of the resource at the bank site.
- The bank during the period of contract, due to its operational requirements, reserves the right to:
  - Change the shift timings of the deployed resources.
  - Increase the number of resources as per the contracted rate OR decrease the number of resources if workloads reduce due to any reasons. The payment for such resources would be paid on pro-rata basis.
  - Shift the operations of management / monitoring (being carried out by L1, L2 & L3 resources) to alternate location (inter / intra city) wholly or partially.
  - In case of inter-city shifting, the shortlisted bidder to provide the resource at the alternate location without any additional cost to the bank. However, prior to shifting notice period of at least 60 days would be given.
- A resource shall be considered absent if allowed leave of absence has already been availed for the month and no standby resource has been arranged by the service provider.
- In addition to the service window indicated as against each service vertical, depending on the bank's requirements the services may be occasionally required on bank holidays/ Sundays/ Gazetted Holidays and beyond the specified service window. Provision must be built by the bidder to provide these occasional services without any additional cost.
- Necessary stand-by arrangements have to be made during absence of any regular staff on account of leave or any other reason.
- Frequent change of staff will not be acceptable. In case of unavoidable circumstances, change of staff must be done with prior approval of SIDBI.
- Service provider and all the deployed staff members will be required to sign the declaration form as per bank's IT security policy or any other similar guideline issued by the Bank.
- In case of disaster at bank's Mumbai data centre, service provider may be required move /provide additional key staff members at SIDBI's DR site (currently Chennai) to manage the DR operation on temporary basis till the data centre at Mumbai is made operational. However, SIDBI will bear expenditure on actual towards to and fro journey of the key staff members of the service provider for the said purpose and also make stay arrangement at bank's guest house or similar other location for them.
- Staff members deployed by service provider will be subjected to the disciplines, office decorum, etiquettes, good behaviour as applicable to any other staff member of the bank.
- Deployed staff members have to make their own arrangement of transport for discharging their duties.

- Staff members deployed by the service provider have to make their own arrangement of lunch/ snacks/ breakfast etc. Alternately, same facility may be availed at bank's lounge at a cost, as charged by the caterer. The decision of the Bank in this regard shall be final.
- In case of services of an existing staff are withdrawn / terminated by the service provider, at least 45 days' notice has to be given by the vendor with at least 30 days overlapping period for proper take-over /hand over of the desk. Any short fall in notice period will be treated as absence of respective staff member.
- Staff deployed by the service provider shall never be deemed to be appointed by the bank nor shall they be under its service conditions.

6.8.4 Statutory & Regulatory Compliance

1. The bidder should ensure all statutory and regulatory compliances towards:
    - **ESIC & EPFO** – All bidders have to ensure that the resources deployed at SIDBI sites are compliant as per the guidelines of ESIC & EPFO. Please note that these are Government bodies, compliance to which is Mandatory.
    - **Minimum Wages Act** – The bidder also has to ensure that they are compliant to the Minimum Wages Act for deployment of resources across SIDBI sites nationwide. The bidder should follow all payout norms as per the Minimum Wage Act (MWA) in all the states.
    - Any other Act/Statutory and regulatory compliances as applicable.
2. The service provider shall at all times guarantee payment of wages not less than that prescribed under the Minimum Wages Act or any notifications passed thereunder and comply with the applicable labour laws in force and give an undertaking to that effect. It shall be the responsibility of the service provider to ensure all labour law compliances with respect to the manpower deployed by it and shall keep the Bank indemnified against all claims, if any, arising from such manpower deployed by it or by any third parties or any authorities etc., arising out of the contract awarded in respect of the present tender.
3. The service provider shall be solely responsible for the redressal of grievances, if any, of its staff deployed in the Bank. The Bank shall, in no way, be responsible for settlement of such issues whatsoever.
4. The Bank shall not be responsible for any financial loss or any injury to any of the staff deployed by service provider in the course of their performing the functions/duties, or for payment towards any compensation. The Bank shall have no liability in this regard.
5. At any stage during the contract period, if the Bank on behest of any statutory authority or RTI query, advises the Service Provider to submit confirmation on the compliance to any or all of the above mentioned, but not limited to, provisions/ Acts,

Service Provider shall submit the same along with requisite details within the time limit as advised by the Bank.

❄ ❄ ❄ ❄ ❄ ❄

7. Service Level Requirement and Liquidity Damages

7.1 Statement of Intent

The aim of this agreement is to provide a basis for close co-operation between SIDBI and the Successful Bidder, for support services to be provided to SIDBI, thereby ensuring that timely and efficient support services are available to SIDBI end-users. The objectives of this agreement are detailed below in Section 7.2.

This agreement is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels.

7.2 Objectives of Service Level Agreements

1. To create an environment which is conducive to a co-operative relationship between the bidder and SIDBI to ensure the effective support of end users.
2. To document the responsibilities of all parties taking part in the Agreement.
3. To ensure that the SIDBI achieves the provision of a high quality of service for end users with the full support of the bidder.
4. To define the commencement of the agreement, its initial term and the provision for reviews.
5. To define in detail the service to be delivered by the bidder and the level of service which can be expected by SIDBI, thereby reducing the risk of misunderstandings.
6. To institute a formal system of objective service level monitoring ensuring that reviews of the agreement is based on factual data.
7. To provide a common understanding of service requirements/capabilities and of the principle involved in the measurement of service levels.
8. To provide for all parties to the Service Level Agreement a single, easily referenced document which caters for all objectives as listed above.

7.3 Period of Agreement

This agreement shall be for a period of 05 years commencing on the date as specified in the **'Master Service Agreement'** to be signed between SIDBI and the Service Provider following the completion of selection process and will continue until end of the contract period or terminated whichever is earlier.

After expiry of the contract period of 05 years, contract may be extended for a period of **01 year** or part thereof on the same terms and conditions.

7.4 Representatives

SIDBI and the Service provider will nominate the representatives responsible for the monitoring and maintenance of the service agreement.

7.5 Management of SLA

Service Level requirements will be necessarily managed by the Service Provider using the existing **HP Service Manager Software (SM 9) or any other tools as advised by the Bank during contract period**. Service provider will make this information available to authorised SIDBI personnel through on-line browsing and also through submission of hard copies of the reports as per requirement.

Service provider will also configure and maintain SLA for 3rd party vendors/ service providers using the same tools.

Compliance of SLA with the service provider will be measured monthly as per details given below. Service window mentioned here refers to ‘**Hours per day’ X ‘Days per week’**.

7.6 Service Level Monitoring

The success of service level agreements depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

Service factors must be meaningful, measurable and monitored constantly.

Service level monitoring will be performed by the Service provider. Reports will be produced as and when required and forwarded to SIDBI.

Service level monitoring and reporting is performed on response times for faults as defined at following sections.

7.6.1 Managed Services

Managed Services would include all service under following heads:

- Data Centre / Disaster Recovery services
- Application Support services / EOD services / Help Desk

7.6.2 Service Level definition

Depending on the criticality and severity of calls, service levels are defined as follows:

Severity Level	Severity Type	Definition
S1	Critical Problems	A problem that affects **entire bank / network or > 80% of the users** of the bank e.g. Outage of Data Center Services viz. Server, Application(s), Internet, Mail System, Database, Severe Virus attack etc.
S2	Major Problems	A problem that affects **a particular office**. e.g. Failure of Network Connectivity, Virus on many devices, Local File/ Mail Server.

S3	Moderate Problems	A problem that affects a **typical user group** e.g. Failure of a department or a floor, an application meant for a particular department or user group etc.
S4	Minor Problem	A problem that affects **a particular user**

7.6.3 Service Level Targets

Following table defines Service Level Targets for Response and Resolution time.

Severity Level	Response Time	Resolution Time	Calculation Window
S4	60 min	6 hrs	Monthly
S3	30 min	4 hrs	
S2	15 min	2 hrs	
S1	**15 min**	**1 hrs**	

7.6.4 Service Level Compliance

The Service Provider needs to ensure following compliance level for each of the Service Levels.

Severity Level	Required Compliance Level			
	Quarter-1		Quarter-2 onwards	
	Response time	Resolution time	Response time	Resolution time
S1	96%	97%	97%	98%
S2	94%	96%	96%	97%
S3	93%	95%	94%	96%
S4	93%	95%	94%	96%

7.6.5 Measurement Metrics

Actual Response and Resolution time will be measured as follows:

$$\textbf{Response time } (\%) = \frac{\textbf{Calls attended within stipulated response time}}{\textbf{Total number of calls received in the month}} \textbf{ X 100}$$

$$\textbf{Resolution time (\%) =} \frac{\textbf{Calls closed within stipulated resolution time}}{\textbf{Total number of calls received in the month}} \text{ X 100}$$

7.6.6 Liquidity damages Calculation

1. Actual vs targeted compliance level for each of the respective service areas will be measured separately in every month.
2. Shortfall in achieving SLA compliance, if any, will be calculated on the monthly basis.
3. For Liquidity damages calculation, Monthly cost of services will be arrived based on proportionate monthly of the corresponding quarterly cost as under:

[Monthly cost = (Total services Cost for respective service area for the quarter) / 3]

4. Liquidity damages for the month will be calculated as:

Liquidity damages amount = **Liquidity damages (%)** X **Monthly Cost**

5. Applicable Liquidity damages (%) would be as under:

Shortfall in SLA Target/Compliance by	Liquidity damages (%)
<= 1 %	1
> 1% and <= 3 %	3
> 3% and <= 5 %	5
> 5% and <= 6 %	6
> 6% and <= 8 %	8
> 8%	10

6. However, the aggregate penalties that may be levied in a month towards the aforesaid managed services shall be limited to 10% of the monthly cost of the Managed Services.
7. Downtime of services on holidays or scheduled downtime will not be considered for calculation of compliance level and liquidity damages.
8. Service provider will make all this information available to SIDBI.
9. The SLA for Application Support Services, EOD Services and Application Software Tools Management shall be applicable **w.e.f. December 01, 2021**. However, the Service Provider shall start extending these services along with other services as per SOW **w.e.f. November 01, 2021**.

7.6.7 AMC Services

Service level monitoring of all the AMC services would be subject to the Service Levels defined below:

7.6.7.1 Service Level Definition and Compliance

Hardware Type	Resolution Time	Compliance Level	Calculation Window
Intel Servers (Windows/ Linux)	6 hrs CTR (Call-to-resolution)	97%	Monthly

Note: Standby of similar or higher configuration item will be deemed as call closure

7.6.7.2 Measurement Metrics

Actual Response and Resolution time will be measured as follows:

$$\textbf{Performance (\%)} = \frac{\textbf{Calls closed within stipulated resolution time}}{\textbf{Total number of calls received in the month}} \times 100$$

7.6.7.3 Liquidity damages Clauses for AMC Services

1. Compliance level towards AMC will be measured monthly.
2. Monthly shortfall in SLA, if any, for the respective category shall be aggregated for the quarter.
3. Liquidity damages for the quarter will be calculated as:
   [**Liquidity damages (%) x AMC Cost for the Quarter]**
4. Applicable Liquidity damages (%) would be as under:

Shortfall in SLA Target/Compliance by	Liquidity damages (%)
<= 1 %	1
> 1% and <= 3 %	3
> 3% and <= 5 %	5
> 5% and <= 6 %	6
> 6% and <= 8 %	8
> 8%	10

5. Liquidity damages towards AMC will be limited to the maximum 10% of the quarterly amount payable towards AMC services. This will be in addition to the liquidity damages charges levied for services mentioned in section of '**Managed Services'** above.
6. Downtime on holidays or scheduled downtime will not be considered for calculation of uptime and liquidity damages.
7. Service provider will make all this information available using the specific SLA tool being used by SIDBI.

7.6.8 Human Resources

Although this project is SLA based, the bidder is required to propose and maintain a minimum level of resource count in each of the service area throughout the contract period. The service provider shall deploy manpower resources as per staffing requirement prescribed in this document. Service provider shall ensure the availability of resources as per defined Service Window for each resource category.

Monthly applicable liquidity damages in the event of absence of manpower resources beyond permissible limit would be as under:

1. **Leave of absence**: Each on-site resource shall be granted a maximum up to 01 (One) day leave per month.
2. Any absence beyond the prescribed leave of absence shall attract a liquidity damages as under in case no substitute is arranged by the Service Provider as per defined requirement:

Allowed leave of absence per month	**Liquidated damages beyond leave of absence**	
	where continuous leave of absence <= 10 working days	**where continuous leave of absence > 10 working days**
01 day	• 110 % of the Man Day cost	• 120% of the Man Days cost

E.g.: If Resource is absent for 13 days (over and above allowed one day leave) in a month, for all 13 days, liquidated damages would be calculated as 120% of Man Day Cost*13.

Note:

1. Un-availed leave (if any) will carry forwarded to next month. In case of change of resource, un-availed leave by earlier resource will lapse and not be carried / clubbed with new resource.
2. Man-day Cost shall be calculated on pro-rata basis by taking man-month rate (22 days in month) for respective resource into consideration.

7.7 Disclaimer

1. In case service provider fails to achieve targeted compliance level of services successively in two quarters or any three quarters in a financial year, SIDBI will reserve the right to re-look at the contract and redefine Service level requirement and liquidity damages clauses to safeguard its interest.
2. SIDBI reserves the right to carry out an annual review of the contract in terms of quality of services, adherence to the SLAs and other obligations of the Service Provider as per provisions of the contract.
3. As part of the annual review, SIDBI may re-validate the Service Provider's financial and technical strength so as to be able to continue to deliver the services as per terms of the contract. In this regard, SIDBI may advise the Service Provider to re-submit its latest financial or any other statement, as submitted by the Service Provider at the time of bidding in this RfP to claim its eligibility.

❄ ❄ ❄ ❄ ❄ ❄

8. Terms and Conditions

8.1 General

1. The Bidders are expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required as in the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

2. Information provided in this RfP is organized in several sections to bring clarity and help the reader to understand quickly. However, Bidder must take into consideration each and every line of this RfP document as a whole while responding. Bidder must get the doubts, if any, clarified by SIDBI before submitting the responses. The bids submitted should be complete in all respect meeting all deliverables under the project. It will be sole responsibility of the selected bidder to deliver each and everything as per the scope of the project during the contracted period. SIDBI shall not be responsible in case of bidder's failure to notice any information, any requirement is underestimated, not understood or any requirement is not interpreted in right manner during preparation/ submitting the response.

3. Unless expressly overridden by the specific agreement to be entered into between the Bank and the successful Bidder, the RFP shall be the governing document for arrangement between the Bank and the Bidders.

4. At any time prior to the deadline for submission of bids SIDBI may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidder(s), modify the RfP by amendment and same will be placed on the Bank's website (www.sidbi.in) and Central Public Procurement (CPP) portal (eprocure.gov.in) for information of all prospective Bidders.

5. All such amendment shall become part of the RfP. The Bidders are required to have a watch on Bank's website and CPP portal for any such amendments till the last moment before submitting the bid.

6. SIDBI shall be under no obligation to accept the lowest or any other offer received in response to this RfP and shall be entitled to reject any or all offers including those received late or incomplete offers without assigning any reason whatsoever. SIDBI reserves the right to make any changes in the terms and conditions of purchase. SIDBI will not be obliged to meet and have discussions with any Bidder, and / or to respond to any representations.

7. SIDBI reserves the right to extend the date for submission of responses to this document with intimation on the Bank's website and CPP portal.

8. Unless agreed to specifically by the Bank in writing for any changes to the RFP issued, the Bidders' responses would not be incorporated automatically in the RFP document.

9. SIDBI reserves the right to change the required specifications and ask for the revised bids or cancel the process without assigning any reasons.

10. The scope of the proposal shall be on the basis of single point responsibility of the bidder, completely covering the delivery of services as specified under this RfP, on end-to-end basis.

11. Bidder must be ready to accept the extension of the contract for a further period of maximum of 1 year or part thereof on the same terms and conditions, if so desired by SIDBI.

12. The Bidder shall promptly notify SIDBI of any event or conditions, which might delay the completion of implementation work in accordance with the approved schedule and the steps being taken to remedy such a situation.

13. Depending on requirement, SIDBI may decide to move any of its offices, Data Centre, Disaster Recovery Site, hardware items, on-site resources deployed under this RfP to any of its other / third party locations during the contract period. Service provider will continue to provide the respective services covered under this RfP at the new location without any extra cost.

14. The Bidder/Service provider is obliged to give sufficient support to SIDBI's staff, work closely with SIDBI's staff, act within its own authority, and abide by directives issued by SIDBI in terms of the Contract. The Service provider is responsible for managing the activities of its personnel and any sub-contracted personnel, and will be solely responsible for any misdemeanors.

15. The Bidder appointed under the RFP shall have the prime responsibility for fulfilling all obligations and providing all deliverables and services required for successful implementation of the Project, notwithstanding the fact that the Bidder may after receiving written confirmation of the Bank, appoint / procure services of third party suppliers to perform all or part of the obligations contained under this RFP, notwithstanding the fact that the Bank, if it deems fit, may for convenience enter into arrangements, including tripartite agreements, with such third party Bidders if required.

16. The Service provider's selection under this RfP document is on the understanding that this RfP contains only the broad provisions for the entire assignment. The Service provider shall be required to undertake to perform all such tasks, render requisite services and make available such resources on-site as may be required for/ incidental to the successful completion of the entire assignment.

17. Bank shall be responsible for timely site readiness in terms of making seating arrangements at respective locations, providing desktops and necessary system

accesses etc. Bank agrees that Bidder shall not be in any manner liable for any delay arising out of Bank's failure to make the site ready.

8.2 Definitions

In this document, the following terms shall be interpreted as indicated:

1. "The Bank", "the bank", "SIDBI", "Purchaser", "Buyer" means Small Industries Development Bank of India (SIDBI);
2. "RFP", "Tender", "RfP", "Bid document' means the 'Request for Proposal document.
3. "Bid" may be referred to as 'Offer'.
4. "Bidder" or "bidder" means the respondent to the RFP document.
5. "Vendor", "VENDOR", "Supplier", "Service Provider" "Seller" means the success bidder selected after successful completion of this RFP.
6. "The Contract" means the agreement entered into between the Bank, represented by its Head Office / Regional Offices/ Branch Offices and the successful Bidder selected after successful completion of the tendering process of this RfP, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein;
7. "The Contract Price" means the price payable to the successful bidder under the Contract for the full and proper performance of its contractual obligations;
8. "TCC" means the Terms and Conditions of Contract contained in this section;
9. "The Project Site" means Small industries Development Bank of India, Mumbai Office.

8.3 Clarification of Bids

1. During evaluation of Bids, the Bank, at its discretion, may ask the Bidders for clarifications of their Bids. The request for clarification and the response shall be in writing (e-Mail/letter), and no change in the price of substance of the Bid shall be sought, offered or permitted.
2. Bidder to submit point by point compliance to the technical compliance and it should be included in the Bid.
3. Bidder to quote for entire project on a single responsibility basis for the services it proposes to offer under the contract.

8.4 Amendment to the bidding document

1. At any time prior to the date of submission of Bids, the Bank, for any reason, may modify the Bidding Document, by amendment issued in the form of corrigendum(s)/ addendum(s).

2. All such corrigendum(s)/ addendum(s) and clarifications, if any, will be posted on Banks website (www.sidbi.in) and CPP portal (eprocure.gov.in) only and it will become part and parcel of RfP.No individual communications would be made in this respect.
3. Interested Bidders are advised to check the Bank's website regularly till the date of submission of bid document specified in the '**Critical Information**' Section including extended date, if any, and ensure that clarifications / amendments issued by the Bank, if any, have been taken into consideration before submitting the Bid. Such amendments/ clarifications/ changes/addendums, if any, issued by the Bank will be binding on the participating Bidders. Bank will not take any responsibility for any such omissions by the Bidder.
4. In order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, the Bank, at its discretion, may extend the deadline for the submission of Bids.

8.5 Governing Language

5. The bid prepared by the Bidders as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be written in English.
6. The contract/ agreement to entered between the Bidder and the Bank subsequent shall be written in English.

8.6 Sub-Contracting

In general subcontracting is not allowed under this RfP, however the bidder may subcontract only for providing AMC Services for specified hardware items, if required. However, in this case SIDBI will only deal with the bidding Bidder, who will be responsible for delivery of all services and is here and after called as the "Prime Bidder". The Prime Bidder will be fully responsible to SIDBI for execution of the contract in its entirety and compliance of SLA.

1. The Prime Bidder will be responsible for the delivery of all the services as per scope.
2. In case of any commercial or legal matter, SIDBI would deal with the Prime Bidder only.
3. In the case of a subcontracting, the responsibility for the details presented in the responses will be of the Prime Bidder. The prime Bidder will be totally responsible for end-to-end delivery of services and will be a single point of contact.
4. The responsibility for the commercial bid lies with the Prime Bidder.

8.7 Rules for Responding to the RFP

1. The responses to the RfP would be deemed to be legal documents and will form part of the final contract. Bidders are required to attach a **'Letter of competence'** as per **Annexure-VII**, from an authorized signatory attesting their competence and the veracity of information provided in the responses. Unsigned responses would be treated as incomplete and are liable to be rejected.

2. Bidders shall have the opportunity to clarify doubts pertaining to the RfP, if any, in the pre-bid meeting. All questions/ queries should be received by the point of contact not later than the date and time mentioned in **'Critical Information'** section of this RfP document. Responses to queries and any other corrections/ amendment will be made available on bank's website and CPP portal. Name of the Bidder, which posed the question, will remain anonymous.
3. Any part of the response either technical or commercial bid, submitted by the bidder cannot be withdrawn / modified after the last date for submission of the bids unless otherwise asked by the bank.
4. SIDBI reserves the right to call for any additional information and also reserves the right to reject the proposal of any Bidder if in the opinion of SIDBI, the information furnished is incomplete or the Bidder does not qualify for the contract.
5. The Commercial and Technical bids will have to be signed on all pages of the bid by the authorised signatory. Unsigned bids would be treated as incomplete and would be rejected.
6. The Bidder must submit the response exactly in the formats mentioned in this RfP and same should be to the point. It must not provide any irrelevant additional information. All the credentials, claimed in the response, must be accompanied with necessary proof. SIDBI would be at discretion to reject the response of the bidder in case any part or whole of the response document is found to be partially or fully incomplete or confusing or misguiding or unverifiable or having irrelevant additional information.
7. By submitting a proposal, the Bidder agrees to promptly contract with SIDBI for any work awarded to the Bidder. Failure on the part of the awarded Bidder to execute a valid contract with SIDBI within stipulated time will relieve SIDBI of any obligation to the Bidder, and a different Bidder may be selected.
8. Any additional or different terms and conditions proposed by the Bidder would be rejected unless expressly assented to in writing by SIDBI.
9. Responses received after the due date / time would be considered late and shall not be accepted or opened. Late received bids shall be returned un-opened within 02 weeks from the bid submission date.
10. SIDBI would not assume any expenses incurred by the Bidder in preparation of the response to this RfP and also would not return the bid to the Bidder.
11. SIDBI shall not be liable for costs incurred during any discussion on proposals or proposed contracts or for any work performed in connection therewith.
12. The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information / description of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "offered", "noted", "as given in brochure / manual" is not acceptable. SIDBI

may treat proposals not adhering to these guidelines as unacceptable and thereby the proposal may be liable to be rejected.

13. Responses received and opened by SIDBI shall become property of SIDBI and can't be returned. Information provided by each Bidder will be held in confidence, and will be used for the sole purpose of evaluating a potential business relationship with the Bidder.
14. The Bidders shall adhere to the terms of this RfP document and shall not deviate from the same. If the Bidders have absolutely genuine issues only then should they provide their nature of non-compliance to the same in the format provided separately with this RfP. The Bank reserves its right to not accept such deviations to the Tender terms, in its sole and absolute discretion, and shall not be obliged to furnish any reason for exercising such right.

8.8 Bid Security & Performance Guarantee

8.8.1 Bid Security / Earnest Money Deposit (EMD)

1. All the responses must be accompanied by a refundable interest free security deposit of requisite value specified in "**Critical Information**" section of the RfP. Bids received without EMD in proper form and manner shall be considered unresponsive and rejected.
2. Request for exemption from EMD (Security Deposit) will not be entertained. However, bidders possessing valid MSE / Udyog Aadhaar Memorandum and Startups are exempted from submission of EMD on submission of proof.
3. EMD should be submitted/ deposited in the form of:

a) Demand Draft / Banker's Cheque from a Scheduled Commercial Bank in favour of "**Small Industries Development Bank of India**" payable at Mumbai.

OR

b) Bank guarantee (BG) from a Scheduled Commercial Bank valid till the bid validity period from the last date of submission of bid and with an invocation period of 03 months beyond the BG validity date, strictly in the format as prescribed in **Annexure– XV**.

OR

c) EMD may be deposited directly in following SIDBI's Bank A/C and copy of e-receipt should be submitted along with documents. SIDBI's Bank A/C Details are as under:

Account Name	Small Industries Development Bank of India
Bank	State Bank of India
Branch	Bandra Kurla Complex, Mumbai - 400051
Type of Account	Current Account

A/C No.	37823159064
IFSC Code	SBIN0004380

d) Any bid received without EMD in proper form and manner shall be considered unresponsive and rejected.

e) Request for exemption from EMD (Security Deposit) will not be entertained.

4. The EMD amount / BG of all unsuccessful bidders would be refunded immediately upon happening of any the following events:
   a) Issue of LoI / Purchase Order (PO) to the successful bidder **OR**
   b) The end of the bid validity period, including extended period (if any) **OR**
   c) Receipt of the signed contract from the selected Bidder; **whichever is earlier.**
5. Successful Bidder will be refunded the EMD amount / BG only after acceptance of the solution by SIDBI and submission of Performance Bank Guarantee by the bidder.
6. ~~In case the acceptance of the solution is delayed due to any reasons beyond the bank's purview, successful bidder shall have the BG towards EMD, validity extended for a period of three months till the equipment is accepted by the bank.~~ **[Clause deleted]**
7. The bid security (EMD) may be forfeited:
   a) If a Bidder withdraws its bids during the period of bid validity.
   b) If a Bidder makes any statement or encloses any form which turns out to be false/ incorrect at any time prior to signing of the contract.
   c) In case of successful Bidder, if the Bidder fails to accept the LOI / Purchase order or sign the contract or fails to furnish performance guarantee.
   d) In all the above cases, the bidder would also be banned for a period of 3 years from subsequent bidding in any of the Bank's (SIDBI) RFP / Tenders.

8.8.2 Performance Bank Guarantee (PBG)

1. The successful Bidder shall provide an unconditional and irrevocable performance bank guarantee in the form and manner provided by the Bank equivalent to **10%** of the total contract value from a scheduled commercial Bank. The performance guarantee will be valid till at least three months beyond the expiry of the contract period and with an invocation period of 03 months beyond the BG validity date. The performance security is to be submitted within ONE month from the date of award of contract as per the format provided by Bank.
2. In the event of non-performance of obligation or failure to meet terms of this RfP/ Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder.

~~3. In case of expiry of BG prior to project completion, the bidder will be required to renew/ extend the BG for further period as per plan. If the performance bank guarantee is not submitted within the time stipulated by SIDBI, the Bank reserves the right to cancel the order and forfeit the EMD.~~ **[Clause deleted]**

4. The Project will be deemed complete only after the expiry of the contract period including extended period, if any, in normal course or on termination of the contract for any reason.
5. Notwithstanding anything to the contrary contained in the contract, SIDBI shall be at liberty to invoke the Performance Bank Guarantee in addition to other remedies available to it under the contract / order or otherwise if the Successful Bidder fails to fulfill any of the terms of contract / order or commits breach of any terms and conditions of the contract.
6. On faithful execution of contract in all respects, the Performance Guarantee of the Bidder shall be released by SIDBI.
7. If aggregated shortfall in achieving Service Level requirement exceeds 10% in two successive quarters or any three quarters in a financial year, SIDBI will inter-alias, be at liberty to invoke the performance guarantee within the ambit of Section 8.8.2 (5) hereinabove in addition to other remedies available to it under the contract or otherwise.
8. Time shall be the essence of the contract / order, therefore, no extension of time is anticipated, but if untoward or extraordinary circumstances should arise beyond the control of the Bidder, which in the opinion of SIDBI should entitle the Bidder to a reasonable extension of time, such extension may be considered by SIDBI at its sole and absolute discretion, however such extension shall not operate to relieve the Bidder of any of its obligations. SIDBI shall not be liable for any extra financial commitment due to such extension of time. In case of any such extension, the Bidder would be required to extend the validity period of the performance guarantee accordingly.
9. In case the contract is extended beyond the contract period of five years, the Bank will place separate PO for the same. The bidder shall submit PBG for 10% of the PO value valid for the extended period of contract and with an invocation period of three months beyond the extended contract period.

8.8.3 Forfeiture of performance security

1. The Bank shall be at liberty to set off/adjust the proceeds of the performance guarantee towards the loss, if any, sustained due to the bidder’s failure to complete its obligations under the contract. This is without prejudice to the Bank’s right to proceed against the Bidder in the event of the security being not enough to fully cover the loss/damage.
2. In the event of non-performance of obligation or failure to meet terms of this RfP/Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder.

8.9 Procurement Policy on Micro and Small Enterprises (MSEs)

1. SIDBI is governed by provisions of the Public Procurement Policy for Micro and Small Enterprises (MSEs) as circulated by The Ministry of MSME, GoI.
2. These provisions shall be applicable to Micro and Small Enterprises (MSEs) registered with District Industries Centers or Khadi and Village Industries Commission or Khadi and Village Industries Board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises (MSMEs).
3. Such MSEs would be entitled for exemption from furnishing tender fee and earnest money deposit (EMD). In case of any issue on the subject matter, the MSE's may approach the tender inviting authority to resolve their grievances.
4. Agencies/ Bidders desirous of availing exemptions/ preference under above provisions should submit a copy of proof of Registration as MSEs/ and ownership of the same by SC/ST along with the tender/RFP.
5. Bidder is required to inform its MSE status as per prevailing MSE definition, if applicable.
6. The bidder to note that, in the current RfP splitting of order is not applicable.

8.10 Period of Validity of Bids

1. Prices and other terms offered by Bidders must be firm for an acceptance period of **six (6) months** from last date for submission of bids as mentioned in '**Critical Information**' sheet including the extended bid submission date, if any.
2. In exceptional circumstances the Bank may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing. The Bid security and price bid (if applicable) provided shall also be extended by the bidder. Any extension of validity of Bids or price (if applicable) will not entitle the Bidder to revise/modify the Bid document.
3. Bank, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

8.11 Deadline for submission of Bids

1. The bids must be received by the Bank at the specified address not later than date mentioned in **'Critical Information'**, given in the beginning of this document.
2. In the event of the specified date for the submission of bids, being declared a holiday for the Bank, the bids will be received up to the appointed time on the next working day.
3. The Bank may, at its discretion, extend the deadline for submission of Bids by amending the Bid Documents, in which case, all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

8.12 Late Bids

Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank will be rejected and returned unopened to the bidder.

8.13 Modification And/ Or Withdrawal of Bids

1. The Bidder may modify or withdraw its bid after the bid’s submission, provided that written notice of the modification including substitution or withdrawal of the bids is received by the Bank, prior to the deadline prescribed for submission of bids.
2. The Bid modification or withdrawal notice must be on bidder’s letterhead, signed and sealed. A withdrawal notice may also be sent by Fax/email and followed by a signed confirmation copy received by the Bank not later than the deadline for submission of bids.
3. No bid may be modified or withdrawn after the deadline for submission of bids.
4. Bank has the right to reject any or all bids received without assigning any reason whatsoever. Bank shall not be responsible for non-receipt / non-delivery of the bid documents due to any reason whatsoever.

8.14 Opening of Technical Bids by the Bank

1. Bids, received within stipulated time, shall be opened, except for commercial bids, as per schedule given in the ‘**Critical information’** sheet.
2. On the scheduled date and time, bids will be opened by the Bank Committee in presence of Bidder representatives. It would be the responsibility of the bidder’s representative to be present at the time, on the date and at the place specified in the tender document. The bidders’ representatives who are present shall sign the required documents evidencing their attendance and opening of bids in their presence.
3. If any of the bidders or all bidders who have submitted the tender and are not present during the specified date and time of opening, bank at its discretion will proceed further with opening of the technical bids in their absence.
4. The Bidder name, presence or absence of requisite EMD and such other details as the Bank, at its discretion may consider appropriate will be announced at the time of bid opening.
5. Bids that are not opened at Bid opening shall not be considered for further evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

8.15 Preliminary Examinations

1. The Bank will examine the Bids to determine whether they are complete, the documents have been properly signed, supporting papers/ documents attached and the bids are generally in order.
2. The Bank may at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.
3. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding document. For purposes of these Clauses, a substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, insurance, Force Majeure etc. will be deemed to be a material deviation. The Bank's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, without recourse to extrinsic evidence.
4. If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.
5. Bids without EMD / Bid security in the proper form and manner will be considered non-responsive and rejected.
6. The Bidder is expected to examine all instructions, forms, terms and specification in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid.

8.16 Use of Contract Documents and Information

1. The bidder shall not, without the Bank’s prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection with, to any person other than a person employed by the Bidder in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
2. The Bidder will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

8.17 Rules for Evaluation of Responses

1. All the responsive bids will be evaluated as per the procedure detailed in **Chapter-10 - Evaluation methodology.**
2. All the documentary proofs are to be submitted along with the bid in this regard.

3. To assist in the scrutiny, evaluation and comparison of responses/offers, SIDBI may, at its discretion, ask some or all the Bidders for additional information/ clarifications on their offer. The request for such clarifications and the response will necessarily be in writing. SIDBI has the right to disqualify the Bidder whose clarification is not received by SIDBI by the stipulated time or is found not suitable to the proposed project.
4. Bidders are requested to be prepared to demonstrate, through presentations and / or site visits, as part of the final evaluation in accordance with the responses given for the identified requirements, within a week's period after the last date of the submission of proposals, as mentioned in **'Critical Information'** of this document. Accordingly, SIDBI will communicate a date and time to all Bidders. The Bidder will arrange such demonstrations, presentations or site visits at its own cost.
5. SIDBI may appoint an external consultant for evaluation of the bid proposal.
6. Bidders must not present any reference as credential for which it is not in a position to present the verifiable facts/documents because of any non-disclosure agreement with its other customer or any other reason whatsoever. SIDBI would not consider any statement as a credential if same cannot be verified as per its requirement for evaluation.
7. SIDBI may at its absolute discretion exclude or reject any proposal that in the reasonable opinion of SIDBI contains any false or misleading claims or statements. SIDBI shall not be liable to any person for excluding or rejecting any such proposal.
8. Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or affect the relative ranking of any bidder.
9. SIDBI reserves the right to reject any proposal in case same is found incomplete or not submitted in the specified format given in this RfP document. SIDBI would not give any clarification/explanation to the concerned bidder in case of such rejection.
10. SIDBI reserves the right to modify the evaluation process at any time during the Tender process (before submission of technical and commercial responses by the prospective bidder), without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change.
11. SIDBI will award the Contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the best bid, provided further that the Bidder is determined to be qualified to perform the contract satisfactorily. However, SIDBI shall not be bound to accept the best bid or any bid and reserves the right to accept any bid, either wholly or in part, as it may deem fit.

8.18 Contacting the Bank

1. After opening of Bids to the time a communication in writing about its qualification or otherwise received from the Bank, bidder shall NOT contact the Bank on any matter relating to its Bid.
2. Any effort by the Bidder to influence the Bank in its decisions on Bid evaluation, may result in the rejection of the Bidder's Bid.

8.19 Conditional Bids

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained from the bank in writing as pre-bid clarifications.

8.20 Commercial Bid

1. **Bid Currency** – The Bidder is required to quote in Indian Rupees ('INR'/ '₹'). Bids in currencies other than INR may not be considered.
2. **Taxes -** The prices quoted would be inclusive of all prevailing taxes such as GST, sales tax, VAT, custom duties, transportation, out of pocket expenses, lodging and boarding expenses, service tax, Education cess etc., that need to be incurred. No additional cost whatsoever would be paid.
3. **Validity of Bids** - The prices and other terms offered by Bidders must be firm for an acceptance period of six (6) months from date of opening of the commercial bids.
4. While any increase in the rates of applicable taxes or impact of new taxes subsequent to the submission of commercial bid shall be borne by SIDBI, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to SIDBI in its favour. This will remain applicable throughout the contract period.
5. **ATS / AMC** – Bidders to note that SIDBI is having adequate licenses of the EMS tools and all other software products being used in the bank. ATS/AMC of the existing licenses of these tools/ software products would be separately procured by SIDBI as per Bank's policy. However, it will be the bidder's responsibility to use these software for providing services using ITIL framework, maintain inventory and manage the software themselves.
6. It would be bidder's responsibility to identify and factor cost of each and every commercial item mentioned in this RfP document during submission of commercial bids. In case of any such item is left out and noticed after completion of commercial evaluation, the selected bidder (Service Provider) has to provide the services at its own cost. However, if anything is missed out by SIDBI in the RfP document, SIDBI would bear the additional expenditure to avail the services at the rate mentioned in the commercial bids of the Service Provider for similar such item.
7. The Commercial Bid should be as per format mentioned in the RFP. In addition, the break-up of the amount over the five years period also needs to be given as per format given.

8. Item-wise unit cost, wherever asked, must be given as per format. Consideration of commercial bids, not submitted as per requisite format, will be at the discretion of the bank.

8.21 No Commitment to Accept Lowest or Any Offer

1. The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.
2. The Bank will not be obliged to meet and have discussions with any bidder and/ or to entertain any representations in this regard.
3. The bids received and accepted will be evaluated by the Bank to ascertain the best and lowest bid in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever.
4. The bank reserves the right to re-tender or cancel the tendering process at any stage without assigning any reason thereof.

8.22 Arithmetic errors correction

Arithmetic errors, if any, in the price break-up format will be rectified on the following basis:

1. If there is discrepancy between the unit price and the total price, which is obtained by multiplying the unit price with quantity, the unit price shall prevail, and the total price shall be corrected unless it is a lower figure. If the supplier does not accept the correction of errors, its bid will be rejected.
2. If there is discrepancy in the price quoted in figures and words, the price, in figures or in words, as the case may be, which corresponds to the total bid price for the item shall be taken as correct.
3. It the vendor has not worked out the total bid price or the total bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.
4. Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or effect the relative ranking of any bidder.

8.23 Acceptance of the Services

After the transition period, the services will be accepted once all the requisite services deliveries have been commenced and requisite resources as per the agreement has been deployed at respective locations to the satisfaction of SIDBI. Service provider must obtain the signature of acceptance from SIDBI at appropriate time.

8.24 Service Delivery

1. Successful Bidder / Service provider will be required to commence all the services with effect from **November 01, 2021.**

2. To meet SIDBI's requirements, as spelt out in the RFP, the Bidder must have the requisite experience in providing services in the field of Information Technology, the technical know-how, and the financial wherewithal that would be required to successfully set-up the required infrastructure and provide the services sought by SIDBI, for the entire period of the contract.
3. Selected bidder would be issued **'Letter of intent (LOI)'** on final selection and completion of internal approval formalities of the bank. Exercise of signing of contract will be parallel activity. While both the parties will endeavour in signing of contract fast, Service provider must start its activities to commence its services based on the LOI issued and stick to the delivery schedule mentioned in this RfP document irrespective of the date of signing of contract.
4. Project is based on delivery of on-site services at SIDBI's office premises as per defined 'Service Level Agreement' (SLA). Bidder is required to post certain number of resources, not less than minimum number as prescribed by the Bank, under several categories on-site at SIDBI office as per its response to this tender. However, the bidder would be required to augment its resource strength as and when required to meet SLA commitment.
5. In addition to providing services as per service window defined in this RfP document, service provider is required to provide services on Saturdays /Sundays /Holidays in case of urgent requirement of the bank without any extra cost.
6. Service Level Requirement and Liquidity damages in not achieving the same have been described in the 'Service Level Requirement' chapter.
7. The Bidder would align its expertise from its respective backend technology practice/tower/vertical in the organisation to attend any critical technical issue as and when required. These services would be in addition to the resources deployed on-site in SIDBI premises. It may be noted that SIDBI will not allow remote access of its data or systems for attending to any technical problem unless it is categorially approved by the Bank.
8. Service provider must arrange for posting of staff members at respective locations having requisite qualification, experience, skill-set, certification etc. as mentioned in the "**Chapter 6: Project Scope**" of this document.
9. Time is the essence of this RfP/ Contract to be entered with the Successful Bidder, therefore, the Bidder must strictly adhere to the delivery schedule of the manpower and services identified in their proposal. Failure to do so will be considered as breach of the terms and conditions of the contract.
10. The Bidder undertakes to provide appropriate human as well as other resources required, to execute various tasks assigned as part of the project, from time to time.
11. SIDBI reserves the right to stop availing of part of the services anytime during the contract period without assigning any reason thereof, with a prior written notice of **30 days**. Payment of such services shall be made on pro-rata basis till the date of

stopping of the services and any payment made already in advance shall be adjusted from any payments to be made in future.

8.25 Ownership of Delivered Services

1. The selected Bidder, who will be awarded the contract, will hold ownership of its delivery of the services under the contract and be responsible for the services delivered. All the deliverables as per the scope of this RfP will become the property of the Bank.
2. SIDBI shall have the sole ownership of and the right to use, all data that may be in possession of the Bidder or its representative in the course of performing the services under the agreement that may be entered into. All documents, report, information, data etc. collected and prepared by Bidder in connection with the scope of work and submitted to SIDBI will be property of the Bank.
3. The Bidder shall not be entitled either directly or indirectly to make use of the documents, reports given by SIDBI for carrying out of any services with any third parties. Bidder shall not without the prior written consent of SIDBI be entitled to publish studies or descriptive article with or without illustrations or data in respect of or in connection with the performance of services.

8.26 Addition / Deletion of qualified offerings

The intent of this Tender is to establish an initial set of service offerings. The Bank recognizes that, as the use of these services expands, it is possible that additional services and / or service categories will be needed. Accordingly, the Bank may request / demand for additional resources for self and / or its associates / subsidiary concerns. In case of requirement of service delivery for associates / subsidiary, a separate order may be placed by the Bank or associates / subsidiary at the same terms & conditions.

For this purpose, a Change Order Procedure will be followed. Bank may request a change order in the event of actual or anticipated change(s) to the agreed scope of work, services, deliverables and schedules. The Bidder will have to prepare a change order reflecting the actual or anticipated change(s) including the impact on deliverables schedule. The Bidder will be liable to carry out such services as required by the Bank at mutually agreed terms and conditions.

The Bidder will have to agree that the price for incremental services does not exceed the original proposed cost and the Bank reserves the right to re-negotiate the price at the unit rates provided for TCO calculations. The Bank has the right to order as much as it wants at those rates.

All quantities mentioned in this RFP are indicative. The quantities of components to be procured as part of this Tender can be varied by the Bank. This also includes the right to modify the number of branches, extension counters, offices, training centres etc.

8.27 Reverse Transition Plan

Reverse Transition Services are the services provided by the Successful Bidder to Bank during the reverse transition period to facilitate an orderly transfer of the Services to Bank or to an alternate third-party service provider nominated by Bank. Where Bank elects to transfer responsibility for service delivery to a number of Bidders, Bank will nominate a Prime services provider who will be responsible for all dealings with Bidder regarding the delivery of Reverse Transition Services.

The reverse transition period of 60 days shall start from 30 days before the end of the contract period including extended period, if any, and shall continue for a period 30 days beyond the end of the contract period including extended period, if any. In case of termination, the reverse transition period shall start 60 days before the termination date in relation to the 90 day's notice period.

As part of Reverse Transition Services, Bank shall have the right, and Bidder shall not object to or interfere with such right, to contract directly with any Bidder's sub-contractor.

The Reverse Transition Services, to be provided by the Bidder shall include the following:

1. Establish exit management governance and detailed transition plan discussion with the Bank.
2. Identify the resources to execute the exit plan.
3. Construct a list of processes, standards, procedures, manuals, SoPs, Network diagrams, Architecture diagrams, Operational work instructions, all events being monitored and the monitoring frequency, asset inventory and any associated reference material that are employed by the bidder to provision services being rendered under the contract.
4. Construct a list of software, scripts, tools or command procedures required to perform the services.
5. Construct a list of all on-going projects, activities and changes scheduled during transition period.
6. Construct list of various audit activities including ISMS audit undertaken during the contract period and compliance status thereof.
7. Construct a list of existing known errors and their remedial action.
8. Construct a list of open problems pertaining to the services.
9. Construct a full list of assets – hardware, software, licenses etc. under the scope of the contract.
10. Knowledge transfer (KT) and education mechanisms including primary KT and shadow KT.
11. Define and agree data/ information exchange process between all parties.
12. Construct a list of sub-contractors used by the Bidder for maintaining the hardware under this RFP and shall ensure that, if so desired by the Bank, all such sub-contractors shall enter into separate annual maintenance agreements for maintenance of the hardware maintained under this RFP, upon commercially reasonable terms and conditions as available currently to the vender or better than the same.

13. Warranties: All the warranties, if any, held by or in the name of the Bidder shall be assigned or transferred “As Is“ in the name of the Bank. The Bidder shall execute any and all such documents as may be necessary in this regard. The Parties shall return confidential information and will sign-off and acknowledge the return of such confidential information.
14. The Bidder recognizes that considering the enormity of the Assignment, the Transition Services listed herein are only indicative in nature and the Bidder agrees to provide all assistance and services required for fully and effectively transitioning the Services provided by the Bidder under this Tender and subsequent Agreement, upon termination or expiration thereof, for any reason whatsoever.

8.28 Business Continuity

The bidder agrees for the following continuity arrangements to ensure the business continuity of the Bank:

1. In the event of this agreement comes to end on account of termination or by the expiry of the term/renewed term of the agreement or otherwise, the bidder shall render all reasonable assistance and help to the Bank and to any new service provider engaged by the Bank, for the smooth switch over and continuity of the services.
2. In the event of failure of the bidder to render the service, without prejudice to any other right the Bank shall have as per this agreement, the bank at its sole discretion may make alternate arrangements for getting the services from any other source. And if the bank gives a prior notice to the service provider before availing such service from any other alternative source, the service provider shall be liable to reimburse the expenses, if any incurred by the bank in availing such services from the alternative source.

8.29 Payment Terms

1. The bidder will submit the cost details in the specified format mentioned in **Annexure-XVII**. Service provider will be paid in quarterly instalments payable at the end of the quarter. Calculation of the instalments will be as follows:

Sr. No.	Service Type	Total Cost for the respective year	Quarterly Payment (QP)	Remarks
1	All the Managed services including DC/DR, application support etc.	$C_{Services}$	$QP_{Services} = C_{Services} / 4$	$C_{Services}$ is the cost of services for the respective year as given in the commercial bid.
2	AMC	---	$QP_{AMC} = C_{AMC}$	C_{AMC} is the actual AMC cost for the quarter as given in the commercial bid.
3	**Total payment for the quarter**		$QP_{Services} + QP_{AMC}$	

2. 100% of the payable for each quarter will be paid in the subsequent quarter. The service provider will submit invoices at the end of the quarter. The Bank will make the payment within 30 days subject to submission of invoices along with all supporting documents / reports viz. monthly SLA data, attendance record etc. towards delivery of services.

3. Based on the SLA data and attendance records, Bank shall make liquidity damages calculations and advise the Service provider to submit credit note towards the liquidity damages amount as calculated, if any. Bank shall not be liable for any delays in release of payment on account of non-receipt of SLA & attendance data and debit note, if applicable, from the service provider.

4. Payment for any quarter will be made after deducting TDS/other taxes and applicable liquidity damages pertaining to respective quarter.

5. Payment of first instalment will be released only after the acceptance of the services and receipt of Performance Bank Guarantee. In case of delay in commencement of some or all the services, payment will be made on pro-rata basis for the services delivered late.

6. In no event services will be withheld and / or terminated by SP in case of delay / non-payment of any dues payable to the service provider on account of any issues pending for resolution. Such issues will be resolved as per the provision available in RfP.

7. Payment in case of Termination of contract – In case the contract is terminated payment towards services will be made on pro-rata basis, for the period services have been delivered, after deducting applicable liquidity damages, TDS/other taxes and adjusting other pending charges, if any.

8. The payments will be made by SIDBI, Mumbai electronically through RTGS/ NEFT. Vendor is required to submit Bank Mandate Form (as per Annexure-XIII) along with cancelled cheque in original along with the technical bid. In the event of any change in vendor's bank details during the contract period, it would be the vendor's responsibility to submit revised Bank Mandate Form along with cancelled cheque leaf.

9. In addition to the services contracted for the Bank, purchase order may also be issued separately by the subsidiary / associate organization or organization being managed by SIDBI for additional services as per the contracted rates at the same terms and conditions. Towards such orders, the payment will be made by the respective organizations.

10. The Bidder must accept the payment terms as proposed herein by the Bank. The financial bid submitted by the Bidder must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted.

11. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the Bank.

12. TDS as applicable, if any, will be deducted while releasing the payment.

13. All Payments will be made to the Bidder in Indian Rupee only.

14. No advance payment will be made in any case.

15. Payment towards forward transition shall be made along with the payment for the first quarter. Payment towards reverse transition shall be made after the successful completion of the Reverse Transition activity.

8.30 Expenses

1. It may be noted that SIDBI will not pay any additional amount separately towards travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses or any other fees /charges.

2. However, the Bidder may factor such expenses within the total project cost towards travelling, boarding and lodging outside Mumbai, if any, to meet the requirement described in the scope of work.

8.31 Liquidity damages for Default in Services

Liquidity damages clauses have defined as follows for different purposes. All of them are independent of each other and several and cumulative and not exclusive of each other.

1. Liquidity damages charged towards **shortfall in achieving Service Level Requirements** for respective services during the contract period has been defined in **Chapter – 7 'Service level requirement and Liquidity damages'.**

2. Delay in commencement of the services w.e.f. the date as mentioned in **Section 8.24** above, will attract liquidity damages @1% of the cost of respective services, severally and cumulatively and not exclusive of each other, for every week's delay subject to maximum of **10%** of the cost of each of such services being delivered. Fraction of week is to be construed as one full week for arriving at the delay in terms of weeks.

Liquidity damages would not be applicable for delay due to reasons attributable to the Bank and Force Majeure. However, it is responsibility of the selected bidder to prove that the delay is attributed to the Bank or Force Majeure.

Bank reserves the right to adjust the liquidity damages and Liquidity damages, if any, against any amount payable to the bidder or PBG.

8.32 Waiver

No failure or delay on the part of either party relating to the exercise of any right power privilege or remedy provided under this RFP or subsequent agreement with the other party shall operate as a waiver of such right power privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right power privilege or remedy preclude any other or further exercise of such or any other right power privilege or remedy provided in this RFP all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

8.33 Violation of Terms

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

8.34 Taxes and Duties

1. The bidder shall be entirely responsible for all taxes, duties, levies, charges, license fees, road permits, etc. as applicable in connection with delivery of products/services at site including incidental services and commissioning.
2. Providing clarifications/particulars/documents etc. to the appropriate tax authorities for assessment of tax, compliance with labour and other laws, etc. will be the responsibility of the vendor at its cost.
3. **Tax deduction at Source** - Wherever the laws and regulations require deduction of such taxes at the source of payment, the Bank shall affect such deductions from the payment due to the Vendor. 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 in force. Nothing in the Contract shall relieve the Vendor from his responsibility to pay any tax that may be levied in India on income and profits made by the Vendor in respect of this contract.

8.35 Insurance

1. Insurance for the entire IT infrastructure owned by SIDBI as on the date of contract or acquired during the course of contract, shall be taken by the bank as per its own policy.
2. Bank will not be liable for obtaining any insurance on the life of the persons deployed by the service provider for the fulfillment of its obligations under this tender.

8.36 Change in Name of Bidding Company

Normally, the Order will be placed on the successful bidder as per the details given in this document. But, if there is any change in name/ address/ constitution of the bidding Firm/ Company at any time from the date of bid document, the same shall be informed by the bidders to the Bank immediately. This shall be supported with necessary documentary proof or Court orders, if any. Further, if the bidding Firm/Company is undergoing any re-organization/ restructuring/ merger/ demerger and on account such a change the Firm/ Company is no longer performing the original line of business, the same shall be informed to the Bank. There shall not be any delay in this regard. The decision of the Bank to place orders or otherwise under such situation shall rest with the Bank and the decision of the Bank shall be final.

8.37 Taken/ Brought over of Company

Subsequent to the order being placed with SIDBI, in the event of bidder or the concerned OEM being taken/ brought over by another company, all the obligations and execution of responsibilities under the agreement with SIDBI should be passed on for compliance by the new company in the negotiation for their transfer.

8.38 Non-Disclosure Agreement

1. During the contract period, the Personnel of service provider will have access to confidential information of the Bank such as Business Data, IP addresses, device configuration, network architecture, etc. The service provider or its Personnel shall not disclose at any point of time to any other person/third party the information so received and use the same degree of care to maintain the confidentiality of the information as if the information is their own. Also, the service provider may use the information only for serving the Bank's interest and restrict disclosure of information solely to those employees of service provider having a need to know such information in order to accomplish the purpose stated above, advise each such employee, before he or she receives access to information, of the obligation of service provider under this agreement and require such employees to maintain these obligations.

2. In case the selected vendor is extending similar services to multiple customers, vendor shall take care to build strong safeguards so that there is no co-mingling of information, documents, records and assets related to services within the ambit of this RfP and subsequent purchase order.

3. The shortlisted bidder shall submit a non-disclosure agreement as per **Annexure-XII** on non-judicial stamp paper of appropriate value.

4. Violation of NDA will lead to legal action against the vendors for breach of trust, forfeiture of PBG and blacklisting.

8.39 Terms and Termination

The contract shall commence on the effective date and continue for a period of five years thereafter. If so desired by SIDBI, contract may be extended for a maximum period of 1 year or part thereof on the same terms and conditions.

8.39.1 Termination for non-performance / Default

1 Bank may, without prejudice to any other remedy for breach of contract, by giving written notice of 30 days to the bidder, terminate the contract in whole or part on occurrence of any or part of the following events:

a. If the bidder fails to deliver any or all of the services within the period(s) specified in the contract or within any extension thereof granted by the Bank pursuant to conditions of contract;

b. The Selected bidder breaches its obligations under the scope document or the subsequent agreement;

c. Serious discrepancy in the quality of services i.e. if aggregate shortfall in achieving Service Level requirement exceeds 10% in two successive quarters or any three quarters in a financial year, during the contract period.

2 Prior to providing written notice of termination to bidder under this clause, the Bank shall provide bidder with a written notice of 60 (sixty) days' in case of clause 1(b) and 1(c) above, to cure such breach of the agreement/contract. If the breach continues or remains unrectified after the expiry of the cure period, the Bank shall have the right to initiate action in accordance with the above clause (1).

3 The Bank will not bear any compensation for these exits as they are due to non-performance/ default of service provider. The Bank's decision in this regard will be final.

8.39.2 Termination for insolvency, Bankruptcy, Winding-up etc.

Bank may terminate the Contract by giving written notice of 30 days' to the bidder:

1 If the bidder becomes bankrupt or otherwise insolvent.

2 The Selected bidder (i) has a winding up order made against it; or (ii) has a receiver appointed over all or substantial assets; or (iii) is or becomes unable to pay its debts as they become due; or (iv) enters into any arrangement or composition with or for the benefit of its creditors; or (v) passes a resolution for its voluntary winding up or dissolution or if it is dissolved.

In this event termination will be without any compensation to the bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has occurred or will accrue thereafter to the Bank.

8.39.3 Termination for the convenience of bank

Notwithstanding the provisions of the Contract and/or the Bid Documents, the Bank at its sole discretion and without prejudice to any other right or remedy and without assigning any reasons, by written 90 days' notice sent to the bidder, may terminate the Contract, in whole or in part, at any time during the contract period. The notice of termination shall specify the brief reason for such termination, the extent to which performance of the Bidder under and in accordance with the Contract is terminated, and the date upon which such termination becomes effective.

8.39.4 The Selected bidder shall have right to terminate only in the event of winding up of the Bank.

8.40 Consequences of Termination

8.40.1 In the event of termination of the Contract due to any cause whatsoever, [whether consequent to the stipulated term of the Contract or otherwise], BANK shall be entitled to impose any such obligations and conditions as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the selected Vendor shall be obliged to comply with and take all available steps to minimize the loss resulting from that termination/breach, and further allow the Bank or its designated 3rd party Vendor to take over the obligations from the service provider in relation to the execution/ continued execution of the scope of the Contract.

8.40.2 In the event that the termination of the Contract is due to the expiry of the term of the Contract in normal course and the Contract is not further extended by BANK, the Vendor herein shall be obliged to provide all such assistance including knowledge transfer and training to the next successor Bidder or any other person as may be required and specified by the BANK, where the successor(s) is a representative/ personnel of BANK to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a period not exceeding 90 days beyond the term.

8.40.3 The Bidder understands the largeness of this Project and that it would require tremendous commitment of financial and technical resources for the same from the Bidder for the tenure of this Tender and subsequent Agreement. The Parties therefore agree and undertake that an exit at any point (due to expiry or termination of this Tender and subsequent Agreement for any reason whatsoever), would happen only after the completion of the notice period of 90 days, and only after completion of the Bidders obligations under the reverse transition mechanism. During this period of Reverse Transition, the Bidder will have to continue to provide the Deliverables and the Services in accordance with this Tender and subsequent Agreement and will have to maintain the agreed Service levels.

8.40.4 Where the termination of the Contract is prior to its stipulated term on account of a default on the part of the Bidder or due to the fact that the survival of the Bidder as an independent corporate entity is threatened/ has ceased, the Bank shall pay the Bidder for that part of the services which have been authorized by the Bank and satisfactorily performed by the Bidder and accepted by the Bank, up to the date of termination, without prejudice any other rights, the Bank may retain such amounts from the payment due and payable by the Bank to the Bidder as may be required to offset any direct losses caused to the Bank as a result of any act/omissions of the Bidder. In case of any loss or damage due to default on the part of the Bidder in performing any of its obligations with regard to executing the scope of work under this Contract the Bidder shall compensate the Bank for any such direct loss, damages or other costs, incurred by the Bank.

8.40.5 Nothing herein shall restrict the right of BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished and pursue such other rights and/or remedies that may be available to BANK under law or otherwise.

8.40.6 BANK reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the Bank guarantee under this contract.

8.40.7 The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

8.41 Applicable laws

1. The Contract shall be interpreted in accordance with the laws prevalent in India.

2. **Compliance with all applicable laws**: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this Tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees/ officers/ resource/ personnel/ representatives/ agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising therefrom.

3. **Compliance in obtaining approvals/ permissions/ licenses:** The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees/ officers/ resource/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising therefrom and the Bank will give notice of any such claim or demand of liability within reasonable time to the bidder.

4. Any demand for information regarding any of the matters to the extent mutually agreeable under the Agreement called for by the RBI or any other regulatory body shall be promptly responded to. The Service provider should undertake to comply with all the statutory and regulatory requirements under the Applicable Laws in connection with Services including Labour and Industrial Laws. All RBI guidelines on outsourcing shall *ipso-facto* form integral part of the Agreement and should be read as forming part

of the Agreement and the Agreement shall contain a clause that it would stand amended to be in conformity with RBI guidelines or any other guidelines applicable, issued by any other Regulator.

8.42 No Employer-Employee Relationship

1. The selected bidder during the term of the contract and for a period of two years thereafter shall not without the express written consent of the Bank, directly or indirectly:

    a. Recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilise the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering the services in relation to the contract; or

    b. Induce any person who shall have been an employee or associate of the Bank at any time to terminate his / her relationship with the Bank.

2. The selected Bidder or any of its holding/subsidiary/joint-venture/ affiliate/ group/ client companies or any of their employees/ officers/ staff/ personnel/ representatives/ agents shall not, under any circumstances, be deemed to have any employer-employee relationship with SIDBI or any of its employees/ officers/ staff/ representatives/ personnel/agents. Staff deployed by the bidder shall never be deemed to be appointed by SIDBI nor shall they be under its service conditions.

8.43 Rights to Visit

1. All records of the Bidder with respect to any matters covered by this Tender document/ subsequent order shall be made available to SIDBI or its designees at any time during normal business hours, as often as SIDBI deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.

2. SIDBI, including its regulatory authorities like RBI etc., reserves the right to verify, through their officials or such other persons as SIDBI may authorise, the progress of the project at the development /customization site of the Bidder or where the services are being rendered by the bidder.

3. The Bank and its authorized representatives, including regulator like Reserve Bank of India (RBI) shall have the right to visit any of the Bidder’s premises with prior notice to ensure that the data provided by the Bank in connection with the services rendered by the Service Provider under the purview of this RfP or subsequent agreement/ purchase order, is not misused. The Bidder will have to cooperate with the authorized representative(s) of the Bank and will have to provide all information/ documents required by the Bank.

4. The right to visit under these clauses shall be restricted to all books, records and information relevant to the outsourcing arrangement under this tender/ subsequent PO/ Agreement. Visit shall be conducted during normal business hours and on normal working days after informing the bidder in advance.

8.44 Audit

1. The vendor shall allow the Bank, its authorised personnel, its auditors (internal and external), authorised personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the services under tender/ subsequent PO/ Agreement.
2. In case any of the services are further outsourced/ assigned/ subcontracted to other vendors, it will be the responsibility of the vendor to ensure that the authorities /officials as mentioned above are allowed access to all the related places, for inspection and verification.
3. Audit under this clause shall be restricted to physical files related to this arraignment. Audit shall be conducted during normal business hours and on normal working days after informing the bidder in advance.
4. Service provider shall allow RBI or its authorised persons to access the Bank's document, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time as prescribed by RBI or SIDBI. In the event that these are not made accessible to RBI within prescribed reasonable time, Bank shall have the right to recover the amount payable to RBI towards supervisory fees, if any.
5. The bank will also carry out annual review of the contract to ascertain the financial stability of the bidder in addition to the performance and service reliability. The bidder shall be required to submit the audited balance sheet and CA certificate etc. ending respective financial years.

8.45 IPR Infringement

As part of this project bidder/service provider will use software/tool to deliver services. If the deliverables and use of any such software/tool used for such delivery, infringe the intellectual property rights of any third person, bidder/service provider shall be primarily liable to indemnify SIDBI to the extent of direct damages against all claims, demands, costs, charges, expenses, award, compensations etc. arising out of the proceedings initiated by third party for such infringement, subject to the condition that the claim relates to Software/ tool provided by Bidder/Service provider under this project.

8.46 Indemnity

1. The Bidder/ successful bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:

   a. Bank's authorized / bona fide use of the Deliverables and /or the Services provided by Bidder under this RfP document; and/or any subsequent agreement; and/or

   b. An act or omission of the Bidder, employees, agents, subcontractors in the performance of the obligations of the Bidder under this RfP document or any subsequent agreement; and/or

   c. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank; and/or

   d. Breach of any of the term of this RfP document and/or of the agreement to be entered subsequent to this RfP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty by the successful Bidder under this RfP document and/or of the agreement to be entered subsequent this RfP; and/or

   e. Negligence or wilful misconduct, fraudulence activities or gross misconduct attributable to the Bidder or its employees or sub-contractors.

   f. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or

   g. Breach of confidentiality obligations of the Bidder contained in this RfP document; and/or

   h. The use of unlicensed and illegal Software and/or allied components by the successful Bidder

2. The Bidder will have to at its own cost and expenses defend or settle any claim against the Bank that the Deliverables and Services delivered or provided under this RfP document infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trade mark in the country where the Deliverables and Services are used, sold or received, provided the Bank:

   a. Notifies the Bidder in writing; and

   b. Cooperates with the Bidder in the defence and settlement of the claims.

3. The Bidder shall not be liable for defects or non-conformance resulting from:

   a. Software, hardware, interfacing not approved by Bidder; or

b. Unauthorized modification of Software or any individual product supplied under this RfP document, or Bank's failure to comply with any mutually agreed environmental specifications.

c. Use of a deliverable in an application or environment for which it was not designed or not contemplated under this Agreement,

d. Modification of a deliverable by anyone other than Bidder where the unmodified version of the Deliverable would not be infringing.

e. Any loss of profits, revenue, contracts or anticipated savings.

4. The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to the negligence /fraudulent activities of the service provider/ outsourced persons deployed by them and the same shall be recovered from the Service Provider.

5. Indemnity would be limited to court; tribunal or arbitrator awarded damages and shall exclude indirect, consequential and incidental damages. However, indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities for reasons attributable to breach of obligations under this RFP and subsequent agreement by the Bidder.

8.47 Limitation of liabilities

8.47.1 The maximum aggregate liability of Service Provider, subject to **clause 8.47.3**, in respect of any claims, losses, costs or damages arising out of or in connection with this RfP/subsequent contract shall not exceed the total contract value/TCO.

8.47.2 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.

8.47.3 The limitations set forth in **Clause 8.47.1** shall not apply with respect to:

a. claims that are the subject of indemnification pursuant to Clause infringement of third-party Intellectual Property Right;

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

c. damage(s) occasioned by Service Provider for breach of Confidentiality Obligations.

d. 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 applicable to current scope of work.

8.47.4 For the purpose of clause 9.26.3(b) the definition of "Gross Negligence " and "Willful Misconduct" are as follows:

1. **"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.
2. "**Willful 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.

8.48 Vicarious Liability

The selected bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the selected bidder and shall be vicariously liable for all the acts, deeds, matters or things, whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the selected bidder, for any assignment under the contract. All remuneration, claims, wages dues etc. of such employees, agents, contractors, sub-contractors etc. of the bidder shall be paid by the selected bidder alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the selected bidder's employees, agents, contractors, subcontractors etc. The selected bidder shall agree to hold the Bank, its successors, assigns and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of selected bidder's employees, agents, contractors, subcontractors etc.

8.49 Confidentiality

The RFP document is confidential and is not to be disclosed, reproduced, transmitted, or made available in whole or in part by the Recipient to any other person. Bank may update or revise the RFP document or any part of it. The Recipient acknowledges that any such revised or amended document is received subject to the same confidentiality undertaking. The Recipient will not disclose or discuss the contents of the RFP document with any officer, employee, consultant, director, agent, or other person associated or affiliated in any way with Bank or any of its customers or suppliers without the prior written consent of Bank.

This tender document contains information proprietary to the Bank. Each recipient is entrusted to maintain its confidentiality. It should be disclosed only to those employees involved in preparing the requested responses. The information contained in the tender document may not be reproduced in whole or in part without the express permission of the Bank. Disclosure of any such sensitive information to parties not involved in the supply of contracted services will be treated as breach of trust and could invite legal action. This will also mean termination of the contract and disqualification of the said Bidder.

The bidder shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. Bidder shall suitably defend, indemnify Bank for any loss/damage suffered by Bank on account of and to the extent of any disclosure of the confidential information.

No media release/public announcement or any other reference to the RFP or any program there under shall be made without the written consent of the Bank, by photographic, electronic or other means.

"**Confidential Information**" means any and all information that is or has been received by the Bidder ("Receiving Party") from the Bank ("Disclosing Party") and that:

1. relates to the Disclosing Party; and
2. is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential or
3. is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants.
4. without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, specifications or other documents or materials that may be shared by the Bank with the Bidder.
5. "Confidential Materials" shall mean all tangible materials containing Confidential Information, including, without limitation, written or printed documents whether machine or user readable.
6. The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:

    i. Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.

    ii. In maintaining confidentiality hereunder, the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:

        a. Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;

b. Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;

c. Limit access to such Confidential Information and materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the Confidential Information and materials in the manner prescribed in this document; and

d. Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information and materials, in whatsoever form, including any and all copies thereof.

iii. The Receiving Party who receives the confidential information and materials agrees that on receipt of a written demand from the Disclosing Party:

a. Immediately return all written Confidential Information, Confidential materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control;

b. To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;

c. So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any HW or other device in its possession or under its custody and control; and

d. To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of this paragraph have been fully complied with.

iv. The restrictions in the preceding clause shall not apply to:

a. Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this document); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.

b. Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

c. The Confidential Information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this document.

v. The confidentiality obligations shall survive the expiry or termination of the agreement between the Bidder and the Bank.

vi. The bidder is required to execute a **Non-Disclosure Agreement** as per **Annexure-XII**

8.50 Privacy and Security Safeguards

1. SIDBI shall have the sole ownership of and the right to use, all data that may be in possession of the Successful bidder/vendor or its representative in the course of performing the services under the agreement/contract that may be entered into. All documents, report, information, data etc. collected and prepared by bidder in connection with the scope of work submitted to SIDBI will be property of the Bank. The bidder shall not be entitled either directly or indirectly to make use of the documents, reports given by SIDBI for carrying out of any services with any third parties. Successful Bidder shall not without the prior written consent of SIDBI be entitled to publish studies or descriptive article with or without illustrations or data in respect of or in connection with the performance of services".

2. The bidder shall not publish or disclose in any manner, without the Banks prior written consent, the details of any security safeguards designed, developed or implemented by the bidder under this contract or existing at any Bank location. The bidder shall develop procedures and implementation plans to ensure that IT assets leaving the control of the bank (removed for repair, replaced or upgraded) are cleared of all Bank data and

software. The bidder shall also ensure that all subcontractors (if permitted in contract) who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without the Banks prior written consent, the details of any security safeguards designed, developed or implemented by the bidder under this contract or existing at any Bank location.

8.51 Corrupt and fraudulent practice

1. As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the execution of this RfP and subsequent contract(s). In this context, the bidders are requested to note the following:

   a. "**Corrupt Practice**" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.

   b. "**Fraudulent Practice**" means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non- competitive levels and to deprive the Bank of the benefits of free and open competition.

   c. "**Coercive practice**" means impairing or harming or threatening to impair or harm, directly or indirectly, any person or property to influence any person's participation or action in the Bidding Process;

   d. "**Undesirable practice**" means (i) establishing contact with any person connected with or employed or engaged by the Bank with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Bidding Process; or (ii) having a Conflict of Interest; and

   e. "**Restrictive practice**" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Bidding Process

2. The Bank reserves the right to declare a bidder ineligible for a period of three years to be awarded a contract, if at any time it determines that the bidder has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

3. The decision of Bank in determining the above aspects will be final and binding on the all the Bidders. No Bidder shall contact through any means of communication the Bank or any of its employees on any matter relating to its Bid, from the time of Bid opening to the time the contract is awarded. If the bidder wishes to bring additional information to the notice of the Bank, it may do so in writing.

4. Any effort/attempt by a bidder to influence the Bank in its decision on bid evaluation, Bid comparison or contract award may result in rejection of the Bidder's bid and/or blacklisting the Bidder. The Bidder agrees not to hire, solicit or accept solicitation either directly or through a third party from any of the employees of the Bank directly involved in this contract during the period of contract and one year thereafter, except as the parties may agree on the case to case basis.
5. The selected bidder shall ensure compliance of CVC guidelines issued or to be issued from time to time for selection of bidder.

8.52 Resolution of Disputes

1. It will be the Bank's endeavour to resolve amicably any disputes or differences that may arise between the Bank and the Bidder from misconstruing the meaning and operation of the Tender and the breach that may result.
2. In case of Dispute or difference arising between the Bank and a Bidder relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The Arbitrators shall be chosen by mutual discussion between the Bank and the Bidder OR in case of disagreement each party may appoint an arbitrator and such arbitrators may appoint an Umpire before entering on the reference. The decision of the Umpire shall be final.
3. The Bidder shall continue to work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or the umpire, as the case may be, is obtained.
4. Arbitration proceedings 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 English.
5. The Bank Clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain bidder/ prospective bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.
6. Notwithstanding anything contained above, in case of dispute, claim & legal action arising out of the contract, the parties shall be subject to the jurisdiction of courts at Mumbai, India only.

7. Any notice given by one party to the other pursuant to this Contract shall be sent to the other party in writing or by fax and confirmed in writing to the other party's specified address. The same has to be acknowledged by the receiver in writing.

8. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

9. No conflict between Bidder and SIDBI will cause cessation of services. Only by mutual consent the services will be withdrawn.

8.53 Grievances Redressal Mechanism

Bank has a grievances redressal mechanism for its customers and designated grievances redressal officers. The bank would use the same mechanism to address the grievances, if any, of the customers related to the services being rendered within the ambit of this RfP.

8.54 Conflict of Interest

The service provider shall disclose to the Bank in writing, all actual and potential conflicts of interest that exists, arises or may arise in the course of performing the obligation(s) as soon as it becomes aware of that conflict.

8.55 No Set-off, counterclaim and cross claims

In case the Vendor/ Bidder has any other business relationship with SIDBI, no right of set-off, counter-claim and cross-claim and or otherwise will be available under this RfP/ Contract/ Agreement to the Vendor/ Bidder for any payments receivable under and in accordance with that business.

8.56 No third-party rights

No provision of the RfP or the agreement that may be entered into is intended to, or shall, confer any rights on a third-party beneficiary or other rights or remedies upon any person other than the parties hereto; nor impose any obligations on the part of the parties to the agreement towards any third parties.

8.57 Representations and Warranties

In order to induce SIDBI to enter into the Contract/Agreement, the Vendor/Bidder hereby represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

1. That the Bidder has the requisite qualifications, skills, experience and expertise in providing Information and Communication Technology (ICT) and other Service(s) contemplated hereunder to third parties, the technical know-how and the financial where with all, the power and the authority to enter into the RfP/Contract / Agreement and provide the Service(s)/Systems sought by SIDBI.

2. That the Vendor/ Bidder is not involved in any major litigation, potential, threatened and existing, that may have an impact of affecting or compromising the performance and delivery of Service(s) /Systems under the RfP/Contract/Agreement.
3. That the representations made by the Vendor/ Bidder in its bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the RfP/Contract/Agreement and the Bid Documents and unless SIDBI in writing specifies to the contrary, the Vendor/Bidder shall be bound by all the terms of the bid.
4. That the Vendor/ Bidder has the professional skills, personnel and resources/ authorizations that are necessary for providing all such services as are necessary to perform its obligations under the bid and the proposed RfP/Contract/Agreement.
5. That the Vendor/ Bidder shall use assets of SIDBI but not limited to software, licenses, databases, documents, etc. solely for the purpose of execution of its obligations under the terms of the RfP/Contract/Agreement. The Bidder shall however, have no claim to any right, title, lien or other interest in any such asset, and any possession of such assets for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.
6. That all the representations and warranties as have been made by the Vendor/Bidder with respect to its bid and Contract / Agreement, are true and correct, and shall continue to remain true and correct through the term of the Contract.
7. That the execution of the Service(s) herein is and shall be in accordance and in compliance with all applicable laws as amended from time to time and the regulatory framework governing the same.
8. That there are (a) no legal proceedings pending or threatened against Vendor/ Bidder or its team which adversely affect/ may affect performance under this RfP/Contract/Agreement; and (b) no inquiries or investigations have been threatened, commenced or pending against the Vendor/ Bidder or its team members by any statutory or regulatory or investigative agencies.
9. That the Bidder has the corporate power to execute, deliver and perform the terms and provisions of the RfP/Contract/Agreement and has taken all necessary corporate actions to authorize the execution, delivery and performance by it of the RfP/ Contract/ Agreement.
10. That all conditions precedent under the RfP/ Contract/ Agreement have been complied.
11. That neither the execution and delivery by the Vendor/Bidder of the RfP/ Contract/ Agreement nor the Vendor's/ Bidder’s compliance with or performance of the terms and provisions of the RfP/ Contract/ Agreement:
    a. will contravene any provision of any applicable law or any order, writ, injunction or decree of any court or governmental authority binding on the Vendor/ Bidder.
    b. will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any

agreement, contract or instrument to which the Vendor/ Bidder is a party or by which it or any of its property or assets is bound or to which it may be subject or

c. will violate any provision of the Memorandum and Articles of Association of the Vendor/ Bidder.

12. That the Vendor/ Bidder certifies that all registrations, recordings, filings and notarizations of the Contract/Agreement and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the Vendor/Bidder which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract/Agreement have been made.

13. That the Vendor/ Bidder confirms that there has not and shall not occur any execution, amendment or modification of any agreement/contract without the prior written consent of SIDBI, which may directly or indirectly have a bearing on the RfP/Contract/Agreement or Service(s).

8.58 Non-Assignment

Neither the subject matter of the contract nor any right arising out of the contract shall be transferred, assigned or delegated to any third party by Vendor without prior written consent of the Bank

8.59 Force Majeure

1. 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.

2. Successful Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that its delay in performance or other failure to perform its obligations under the contract subsequent to this RfP is the result of an event of Force Majeure.

3. If a Force Majeure situation arises, the Bidder shall promptly notify the Bank in writing of such condition, the cause thereof and the change that is necessitated due to the conditions. Until and unless otherwise directed by the Bank in writing, the Bidder shall continue to perform its obligations under the Contract as far s is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

4. In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, SIDBI and the successful bidder shall hold consultations with each other in an endeavour to find a solution to the problem

5. In the event of the Force Majeure conditions continuing for a period of more than three months the parties shall discuss and arrive at a mutually acceptable arrangement.

8.60 Miscellaneous

1. Bidder is expected to peruse all instructions, forms, terms and specifications in this RfP and its Annexures.

2. Bidder would undertake to provide appropriate human resources, over and above the minimum number of resources prescribed in this RfP, as well as other resources (PC/laptop etc) required, to execute the various tasks assigned as part of the project, from time to time.

3. SIDBI shall not be held liable for additional costs incurred during any discussion on contracts or for any work performed in connection therewith.

4. The offers containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. SIDBI may treat proposals not adhering to these guidelines as unacceptable and thereby the proposal may be liable to be rejected.

5. Bidder shall promptly notify SIDBI of any event or conditions, which might delay the completion of project in accordance with the approved schedule and the steps being taken to remedy such a situation.

6. Bidder shall indemnify, protect and save SIDBI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting directly or indirectly from an act or omission of Bidder, its employees, its agents, in the performance of the services provided by contract, infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided by Bidder as part of the delivery to fulfil the scope of this project.

7. Depending on requirement, SIDBI may decide to move its project site to other locations during the contract period. Bidder will continue to provide the respective services at the new location, if so decided, without any extra cost.

8. Any publicity by Bidder in which the name of SIDBI is to be used should be done only with the explicit written permission of SIDBI.

9. Bidder is obliged to give sufficient support to SIDBI's staff, work closely with SIDBI's staff, act within its own authority, and abide by directives issued by SIDBI that are

consistent with the terms of the order. Bidder is responsible for managing the activities of its personnel, and will hold itself responsible for any misdemeanours.

10. SIDBI reserves the exclusive right to make any amendments/ changes to or cancel any of the above actions or any other action related to this RfP.

11. Personnel engaged by the bidder for performance of its obligations under the work, shall, for all purpose, including applicability of law and welfare enactments, be the employee/staff of the bidder and they shall have no claim to be appointed in the services of the bank. Bidder shall take suitable measures for them in this regard.

❄ ❄ ❄ ❄ ❄ ❄

9. Minimum Eligibility Criteria

Proposals not complying with the 'Minimum Eligibility criteria' are liable to be rejected and will not be considered for further evaluation. The proposal should adhere to the following minimum eligibility criteria.

S. N.	Criteria	Supporting Documents Required
➢ **Incorporation & Operation**		
1	The Bidder should be either a Government Organization/ PSU/ PSE/ partnership firm or a limited Company under Indian Laws or /and an autonomous Institution approved by GOI/RBI promoted.	a. Partnership firm: Certified copy of Partnership Deed **OR** Limited Company: Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. b. Reference of Act/Notification
2	The Bidder should have been in existence in India and must be engaged in the business of Managed services of IT infrastructure in India for at least five years as on 31.12.2020. (In case of mergers / acquisition / restructuring or name change, the date of establishment of the earlier / original partnership firm/limited company will be taken into account).	a. Partnership firm: Certified copy of Partnership Deed. OR Limited Company: Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. b. Reference of Act/Notification c. For other eligible entities: Applicable documents. d. Copy of Work order / agreement along with completion certificate for completed projects.
3	The Bidder should have an office registered in India. One of its offices must be in Mumbai to handle the project smoothly.	a. Self-declaration with address of registered office and local office at Mumbai along with contact details on letterhead of the bidder duly signed by authorized signatory of the bidder.
4	Compliance of Statutory & Regulatory guidelines towards clause # 6.8.4 under Chapter 6: Project Scope.	a. Self-declaration on letterhead of the bidder duly signed by authorized signatory of the bidder.
➢ **Financials**		
5	The bidder should have minimum average annual turnover of INR 200 Crore during any two of the last three financial years ending March 2020, out of Indian Operations. **Note -** In case of MSE bidders, the turnover criteria may be relaxed by 15% subject to meeting the quality and	a. Copy of Auditor certificate for the financial years 2017-18, 2018-19 and 2019-20. b. Copies of last three years' balance sheet. c. Copies of last three years' Profit & Loss Statement.

S. N.	Criteria	Supporting Documents Required
	technical specifications as per RFP.	
6	The bidder should have positive networth and cash profit (i.e. no cash loss) in 2 years out of last 3 years.	
➢ **Experience**		
7	The respondent must have experience of **on-site IT infrastructure management**, similar to scope of this RfP, in All India Public Financial Institutions or Scheduled Commercial Banks / PSUs / Govt. Organizations having at least 50 branches spread across multiple states/regions in India, during last 03 years as on December 31, 2020, where the bidder has set up facilities for centralized management of IT infrastructure at the customer's premises.	a. Relevant credential letters supporting the claim from the respective organization submitted along with contact details of the organization. b. Copy of Work order / agreement along with completion certificate for completed projects.
8	The bidder should have at least following number of customer reference for All India Public Financial Institutions or Scheduled Commercial Banks / PSUs / Govt. Organizations, for projects of similar in nature as to the scope of this RfP: a. 01 Project of order value of 30 crore or more. **OR** b. 02 Projects each of order value of 20 crore or more. **OR** c. 03 Projects each of order value of 15 crore or more.	a. Copy of purchase order / agreement signed between the parties and bidder
9	The bidder must have its own back-end technology Towers/ Verticals/ Service line internally in the organisation for providing support to the on-site team in case of critical technical issues.	a. Relevant details along with contact information of tower/verticals' head must be given in form of certificate.
10	The bidder must be having its own service support centre setup in Mumbai with skilled resources from where the governance of this project shall be carried out.	a. Relevant details along with contact information of service centre must be given in form of certificate.
➢ **Credentials**		

S. N.	Criteria	Supporting Documents Required
11	The bidder should have at least two of the accreditations / certifications out of ISO 9001, ISO 20000, ISO/IEC 27001, ISO/IEC 27002. The bidder must furnish valid certificate copies.	a. Copy of relevant certificates
12	The bidder should not have been black-listed by any Public Financial Institutions, Public Sector Bank, RBI or IBA or any other Government agencies. Bidder must certify to that effect.	a. Self-declaration to this effect on bidder's letter head signed by bidder's authorized signatory as per **Annexure-IV**.
13	The Bidder should submit Pre-Contract Integrity Pact as per format provided in the RfP.	a. Pre-Contract Integrity Pact duly signed by authorized signatory on non-judicial stamp paper of requisite value (to be borne by the bidder) as per format given in **Annexure – XVI** need to be enclosed

Note:

1. The references of the customers must be submitted with official contact details for verification. References which cannot be verified with provided contact details won't be considered as valid evidences.
2. Those who fulfill all the eligibility criteria as mentioned above would be eligible to take part in this bid exercise.
3. Details and corresponding documents as required for all the Technical Parameters stipulated under **Section 10.2.2** should be submitted by Bidders.
4. The fulfillment of above eligibility criteria would be ascertained as of **31.12.2020** unless specified in the clause.
5. All such experience/ references of services must be based on on-site (Customer's premises) service delivery model.

❄ ❄ ❄ ❄ ❄ ❄

10. Evaluation Methodology

10.1 Objective

1. The objective of this evaluation methodology is to facilitate the selection of one Service Provider (SP) ensuring technically superior and professional services at optimal cost.
2. The selected bidder will be entrusted with end-to-end responsibility of handling most critical IT services of the bank for fairly long period of time of five years.
3. The project is based on fixed cost and the selected bidder has to deliver the services with performance level as set out in this RfP document as **'Service Level Agreement' (SLA).**

10.2 Evaluation process

1. The Bank has adopted a Three (3) bid processes in which the Bidder has to submit following bids in separate envelopes at the time of submission of bids as stipulated in this document.
   a. Minimum Eligibility Bid
   b. Technical Bid
   c. Commercial Bids
2. The Bank shall evaluate first the **'Minimum Eligibility Bid'** and based on its evaluation, **'Technical Bids'** shall be undertaken for evaluation at the second stage only for the bidders qualifying the minimum eligibility bid. All **'Commercial bids'** shall be opened in third stage for only the shortlisted bidders out of technical evaluation.
3. The evaluation by the Bank will be undertaken by a Committee of Officials or/and representatives formed by the Bank and its decision will be final.
4. **Normalization** - SIDBI reserves the right to go for normalization process after technical evaluation and accordingly may request all the bidders to submit revised bid (technical or commercial or both) to avoid any possible ambiguity in evaluation process or make apple-to-apple comparison or to bring further transparency in the evaluation process.

10.2.1 Evaluation of Eligibility Criteria

1. Bids submitted by all the bidders would be evaluated for eligibility as mentioned in the '**Minimum Eligibility Bid'** section. Bids not complying with the eligibility criteria as set out in minimum eligibility bid are liable to be rejected and will not be considered for further evaluation.
2. Successful bids out of this stage would be considered for technical evaluation.
3. Bidders must submit the proof of all the credentials as required for evaluation of eligibility criteria. Claims of the bidders without verifiable facts won't be considered as credentials towards satisfying eligibility criteria.

10.2.2 Evaluation of Technical Bids

1. The technical bids will be evaluated for determining the continued eligibility of the Bidders for Project and compliance of the bids with the necessary technical requirements and scope of work of this tender.
2. SIDBI may seek specific clarifications from any or all the Bidder(s) at this stage. All the clarifications received within the stipulated time shall be considered for evaluation. In case satisfactory clarifications are not received from the bidders within the stipulated time, the respective technical parameters would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by SIDBI.
3. Technical bids would be evaluated on the following broad parameters:

SN	Parameters		Weightage %
A	Credentials *		15%
B	Technical Experience *		50%
	(1) DC - DR Services *	40%	
	(2) Application Support Services *	10%	
C	Resource Deployment		20%
D	Reference Feedback		10%
E	Presentation		5%
	Total		**100%**

* Work orders / Assignments having commencement date prior to 1 year with effect from 31/12/2020 will only be considered.

4. The technical bid will be analyzed and evaluated, based on which the **Relative Technical Score (RS_{Tech})** shall be assigned to each bid on the basis of parameters mentioned above.

5. **Relative Technical Score (RS_{Tech})** for each vendor will be calculated as follows based on above parameters:

$$\boxed{RS_{Tech} = T / T_{high} * 100}$$

Where,

RS_{Tech} = Relative score obtained by the bidder
T = Technical score obtained by bidder
T_{High} = Highest Technical score secured among the Bidders

6. Technical Bids receiving a RS_{Tech} greater than or equal to a score of **80** (cut-off marks) will be eligible for consideration in the subsequent round of commercial evaluation.

7. If less than 3 bidders qualify as per above criteria (RS_{Tech}> = 80), SIDBI reserves the right to short list maximum top 3 bidders subject to RS_{Tech}>= 75.

8. Each of the above areas of evaluation is described in detail below based on which scoring will be done.

10.2.2.1 A. Credential

S.N.	Criteria	Documents to be submitted	Criteria	Marks
A.	**Credentials**			**100**
1	**Approach & methodology**			**69**
	Project Management & Governance			30
	1. Understanding SIDBI's requirement vis-a-vis scope of work as defined in the RfP 2. Project organisation; Methodology of proposed governance, Processes defined for Management of the project 3. Plan of project communication 4. Plan of quality management 5. Change control mechanism 6. Risk management/ mitigation strategy	Based on the detailed processes / procedures / approach submitted in the Bid Response	No Clarity — **0** For each area — **5** **Maximum Marks** — **30**	
	Plan of implementation/transition and service delivery management			**24**
	1. Implementation/ Rollout plans/ strategy 2. Plan of transition - Technical transition, Process transition, Resource mobilization, Administrative transition. 3. Strategy of implementation of ITIL based framework of service delivery. 4. Detailed description about capability of Application Support Partner in terms of resources / handing similar assignments supporting multiple applications. 5. Capability in terms of availability of resources / technological experience / processes in meeting the timeline would be taken into account. 6. Bidders approach towards bringing its knowledge, skills and experience for proposed SIDBI project in terms of providing ongoing services.	Based on Bid Response	No Clarity — **0** For each area — **4** **Maximum Marks** — **24**	
	Bidder's capability/competency			**15**
	1. Core competency of the bidder in such on-site outsourcing project as per proposed model of SIDBI, a. DC/DR Managed Services b. Application Support Services c. AMC Services – directly by bidder	Based on Bid Response	No Clarity — **0** For each area — **5** **Maximum Marks** — **15**	
2	**Application Support Credentials**			**31**

	1. No. of applications / business software products in Banking domain supported	Based on Bid Response	No Clarity: 0 For each Application: 2 For CBS: 10 **Maximum Marks: 26**
	2. Providing centrally managed services using the help desk software and handling similar outsourcing project;	Based on Bid Response	No Clarity: **0** **Maximum Marks: 5**
Work orders / Assignments having commencement date prior to 1 year with effect from 31/12/2020 will only be considered.			

10.2.2.2 B. Technical Experience (DC- DR Operations)

S.N.	Criteria	Documents to be submitted	Criteria	Marks
A.	**Technical Experience (DC DR Operations)**			**100**
1	**DC / DR Management - Banking References**			**60**
	Experience in below mentioned domains for providing services in All India Public Financial Institutions or Scheduled Commercial Banks / PSUs / Govt. Organizations having at least 50 branches spread across multiple states/regions in India. • Database management • Server administration (Windows, Linux, Unix) • Mail management • SAN Administration • Enterprise Backup Management • Security management • Management of DR Site	• Copy of Work order / agreement along with completion certificate for completed projects. • Relevant credential letters Supporting the claim from the respective organization submitted along with contact details of the organization.	No project: **0** For each project Reference: **30** **Maximum Marks: 60**	
2	**ITIL Implementation**			**40**
	Number of projects for managing/ implementing ITIL Framework processes viz. Service Operation, Service Transition Service Design, Service Strategy, Continual Service Operation, using ITSM tools.	• Copy of Work order / agreement. Completion certificate for completed projects.- Relevant credential letters Supporting the claim from the respective organization submitted along with contact details of the organization.	No project: **0** For each project reference: **10** **Maximum Marks: 40**	
Work orders / Assignments having commencement date prior to 1 year with effect from 31/12/2020 will only be considered.				

10.2.2.3 B. Technical Experience (Support Services)

S.N.	Criteria	Documents to be submitted	Criteria	Marks
A.	**Experience (Application Support Services)**			**100**
1	**Application Support Management - Banking References**			**80**
	Number of applications supported for any All India Public Financial Institutions or Scheduled Commercial Banks / PSUs / Govt. Organizations each having at least 50 offices across India.	• Copy of Work order / agreement along with completion certificate for completed projects. • Relevant credential letters Supporting the claim from the respective organization submitted along with contact details of the organization.	For each CBS application For each non-CBS application in Banking domain e.g. Loan Management System, Credit Rating Module etc. Any application not covered above **Maximum Marks**	40 20 0 **80**
2	**Help Desk Management - Banking References**			**20**
	Number of projects for Managing Help Desk for All India Public Financial Institutions or Scheduled Commercial Banks / PSUs / Govt. Organizations each having at least 50 offices across India, using Help Desk Software.	• Copy of Work order / agreement. Completion certificate for completed projects. • Relevant credential letters Supporting the claim from the respective organization submitted along with contact details of the organization.	No project reference For each project reference **Maximum Marks**	0 10 **20**
Work orders / Assignments having commencement date prior to 1 year with effect from 31/12/2020 will only be considered.				

10.2.2.4 C. Resource Deployment

S.N.	Criteria	Documents to be submitted	Criteria	Marks
A.	**Resource Planning**			**40**
1	Team Structure proposed for Project Governance	• Self-declaration duly signed by authorized signatory	No Clarity Defined **Maximum Marks**	0 10 **10**
2	Bidder's capability in terms of back-end technical resources to support on-site resources across service areas; Separate Tower available for DBA, WINTEL, VMWare, SAN, Backup,	• Declaration Letter from HR Department in support of the claim.	No Clarity For Each Tower **Maximum Marks**	0 1 **10**

S.N.	Criteria	Documents to be submitted	Criteria	Marks
	Network, Middleware software tools, Mail, LINUX/ Unix, Security			
3	**Team Size**			**20**
	Project team structure; Sizing of the service team for different activities of data centre and helpdesk;	Based on Bid response submitted.	Scoring for bidders for **'Resource Planning'** will be done as follows subject to proper representation in each category; Up to 50 resource – **20** - Anything more than 50 up-to 60 – 6 Anything more than 60 – 0	
	For manpower consideration all the proposed resource should be on the payroll of the Bidding Company.			

10.2.2.5 D. Customer Reference Feedback

S.N.	Criteria		Marks
A	**Customer Feedback**		**100**
1	**General**		**30**
	Overall satisfaction level of customer	30	
2	**Customer Feedback**		**70**
	Type of Client/ Industry (Relevance of client with current expectations) and geographical spread/distribution of the offices of the referred customer.	10	
	Is the vendor providing on-site services using ITIL model?	10	
	Commitment of the bidder towards meeting defined SLAs.	10	
	Efficiency and effectiveness of data centre services	10	
	Efficiency and effectiveness of application support	10	
	Timeliness of providing services and meeting SLAs	10	
	Satisfied with the support offered by the vendor/ Odd hours support/ After office hours support	10	

10.2.2.6 E. Presentation

S.N.	Criteria	Documents to be submitted	Criteria	Marks
A.	Presentation			100
	Explanation of how the services being proposed by the bidder in achieving its objectives			
	Bidder's clarity on the project scope			30
	Transition Management			30
	Service delivery methodology & Project Management			40

10.3 Evaluation of Commercial Bids

1. In this phase, the Commercial Bids of the Bidders, who are found technically qualified in previous phase, will be taken for commercial evaluation.
2. The date for opening of commercial bids will be separately advised.
3. **Relative Technical Score (RS_{Tech})** of the technically qualified bids would be announced before the representatives of the bidders and the commercial bids of those bidders would be opened for commercial evaluation.
4. **Net Present Value (NPV)** would be calculated for the value, quoted for all the five years, to arrive at derived commercial bid value for evaluation. [NPV formula of Microsoft Excel Worksheet shall be used for the purpose].
5. Discount rate will be considered by bank as **8.00%** for calculation of NPV.
6. Total cost of ownership (TCO) for all the bidders shall be arrived as under:

TCO = **SUM [NPV (Yearly Cost of Managed Services & AMC Services for respective years)]**
+ Cost of Reverse Transition
+ Cost of Forward Transition
+ Optional Cost of Resources as per man-month rate

7. The Bidder with lowest **Total Cost of Ownership (TCO)** shall be determined as Lowest Commercial Price (L1) and be short listed for award of contract for Infrastructure Managed Services and Application Support Services for Datacenter (DC) & Disaster Recovery (DR) Site, for a period of Five (05) years.
8. Purchase order with selected L1 vendor shall be placed for the total Cost of Managed Services & AMC Services plus Cost of forward transition and cost of reverse transition. Purchase order for optional resource requirements shall be placed separately on need basis during the contract period.

10.4 Award of Contract

1. The Bank would issue LoI / Purchase order to the shortlisted bidder(s) after completion of above process.

2. The shortlisted bidder/s has to return the duplicate copy of LoI/Purchase order to the Bank within one week from the date of LOI/ Purchase order duly Accepted, Stamped and Signed by Authorized Signatory in token of acceptance.
3. Failure to accept the LOI/ Purchase order within one week from the date of receipt of the LoI/ Purchase order makes the EMD liable for forfeiture at the discretion of the Bank. In such an event, the bidder stands disqualified for further participating in the subject Bid.

10.5 Signing of Contract

1. The selected bidder has to sign a contract with the Bank **within 30 days** from the date of acceptance of the LOI/ Purchase order by the shortlisted bidder, as per the terms and conditions of the RFP on a non-judicial stamp-paper of appropriate value.
2. This initial contract will be called as the "**Master Service Agreement (MSA)**" which will act as the comprehensive contract document between the Bank and the service provider for all purposes/conditions related to the RFP. The MSA will be the permanent reference & the contract document (with subsequent modifications, if any). The modifications to the MSA during the period of contract will be mutually agreed and will be accommodated in the form of addendum/schedules to the MSA since procedural aspects, services etc. will be continuously evolving.
3. The agreement shall include scope of work, all terms and conditions, specifications of RfP, and also the Bill of Material and price as agreed finally after Bid evaluation and negotiation, with references to the clarifications issued by the Bank during the tendering process, responses received from shortlisted bidder, corrigendum/ addendums to the RfP issued, if any, by the Bank.
4. The agreement shall be executed in English language in one original, the Bank receiving the duly signed original and selected service provider receiving the photocopy. The contract agreement shall be valid till all the contractual obligations are fulfilled.
5. All the expenses including stamp duty, levies and other monies payable in connection with the execution of this Agreement shall be borne by the selected bidder only.

❄ ❄ ❄ ❄ ❄ ❄

End of Document