

### Important Dates

#	Particulars	Timeline
5	Last Date of Submission of RFP Response (Closing Date)	25th October 2021 3:00 PM Mode: Online URL: <a href="https://www.tenderwizard.com/BOB">https://www.tenderwizard.com/BOB</a>
6	Eligibility Cum Technical Bid Opening Date	25th October 2021 3:30 PM Mode: Online URL: <a href="https://www.tenderwizard.com/BOB">https://www.tenderwizard.com/BOB</a>

### Addendum to the following Annexures:

#### 1. Annexure 12 – Project Details Scope of Work

All other Terms & Conditions are same as per our RFP no. BCC:IT:PROC:113:40 Dated 13<sup>th</sup> September 2021 for Request for Proposal for Selection of Service Provider for Hosting Bank's Website (Under Opex Model in a Dedicated Infrastructure).

## Annexure 12 – Project Details Scope of Work

### 1. Project Scope

Bank will award the contract to the successful bidder and the bidder should provision of Hosting Bank's centralized corporate website on a dedicated Infrastructure for Servers (as per the specifications) ,Network Switches and shared infrastructure for DDoS services (for clean internet Bandwidth), NIPS (can be combined with firewall), Firewall, Web Application Firewall(WAF), Application Load Balancer (can be combined with WAF),Router along with other solutions such as Network equipment's, Network monitoring tools, SIEM, Backup, PIM, DAM etc should be provided by the bidder as part of their solution.

The Bidder shall perform the following tasks as per Bank requirement and satisfaction as per this RFP, but not limited to:

- i. The selected vendor has to provide a **dedicated Infrastructure for Servers (as per the specifications) ,Network Switches and shared infrastructure for DDoS services (for clean internet Bandwidth), NIPS (can be combined with firewall), Firewall, Web Application Firewall(WAF), Application Load Balancer (can be combined with WAF),Router along with other solutions such as Network equipment's, Network monitoring tools, SIEM, Backup, PIM, DAM etc,**
- ii. The vendor must provide the managed services as mentioned in Annexure 19 for maintaining Bank's website hosted at DC & DR location on 24x7 basis.
- iii. Proposed DC (Primary) must be at Mumbai & DR (Secondary) must be in different seismic zone anywhere within India.
- iv. Proposed DC (Primary) & DR (Secondary) sites should be Tier-3 Data Centres or higher and should be ISO 27001 certified.
- v. The selected vendor to complete the entire job of providing IT Infrastructure within 6 weeks from the date of order placement.
- vi. The selected vendor needs to assist the Bank's team / Bank's identified vendor to host the centralized website for both DC & DR location.
- vii. The vendor must take care of all aspects with regards to the IT Infrastructure required for hosting the Bank's website on dedicated server.
- viii. The vendor must take care of all aspects in Implement network segmentation and segregation. Network segmentation and segregation makes it more difficult for attackers to move laterally within connected networks. For example, placing the web server in a properly configured demilitarized zone (DMZ) limits the type of network traffic permitted between systems in the DMZ and systems in the internal corporate network.
- ix. The hosting of Bank's Website has to be done on the IT infrastructure required as

specified in Annexure - 20 at the vendor's Mumbai location which would be considered as DC & at another location (in different seismic zone) within India as DR.

- x. The vendor must submit the technical specifications for the IT infrastructure such as DDoS, NIPS, Firewall, Web Application Firewall, Application Load Balancer, Router, Switch (if any hardware), Racks, Power source, Air-conditioning unit etc., required to host Bank's website.
- xi. The selected vendor will be responsible for all necessary security measures to be taken to protect website hacking, unauthorized access, viruses, intrusion and attacks from internal and external source/people.
- xii. The selected vendor must provide the documents on DDoS policy, NIPS policy, Web Application Firewall policy, Application Load Balancer policy, Firewall policy, Network Management Policy, Intrusion Detection Policy, Physical Security Policy, DNS Policy, Webserver Policy, Disaster Recovery Policy, Anti-virus Policy, etc., to Bank
- xiii. The selected Vendor must setup the IT Infrastructure must be compatible for IPv6 as well as IPv4. - 13- Servers of the same configuration (as mentioned in Annexure 2) required at both DC – production 6 nos., UAT 1 nos. and DR – production 6 nos.
- xiv. The selected Vendor must setup the failover between DC & DRC, if application / database fails at one location (either DC or DR) the application / database should switch over to another location (DC or DR) as per the RTO / RPO and Bank's corporate website should seamlessly work. Any switch over from DC to DR or vice versa should be seamless and without changing the DNS Entries of Bank's Domain.
- xv. The Vendor must provide the Internet Bandwidth of Minimum 20,000GB/Annum Data Transfer mode.
- xvi. The vendor has to provide additional Bandwidth charges per 100 GB, if the allocated Bandwidth utilization completed.
- xvii. The selected Vendor must submit the Bandwidth usage, availability of website on a monthly basis to the Banks team.
- xviii. The selected vendor has to inform the Bank if any disaster happens at DC or vice versa and also in need of switch over to DR within a time period of maximum 30 Minutes after receiving an approval from the Bank's side for switch over.
- xix. Clause Deleted
- xx. The selected vendor should allow the Bank's Internal / External 3rd Party auditors to audit the proposed setup against the CERT-in guidelines.
- xxi. Bank will inform vendor in advance for the visit of the Bank's Internal / External 3rd Party auditors as and when required during the contract period.

- xxii. The selected vendor must provide the support in terms of website availability through the internet, safeguard against virus attacks on the server and hacking of the website and other website related matters on 24x7 basis.
- xxiii. The selected vendor must provide the web statistics report to Banks on the 1st day of every month and also as and when it is required by the Bank. All the monitoring report should be accessible through a unique URL provided to Bank. Alert the Bank officials within 15 minutes of any type of attacks. Initial response to the incident within 60 minutes with action plan on taking down and other alternative response mechanisms. Resolution of the incident within 180 minutes. The period of availment of Bank's Websites hosting services shall be extendable, based on mutually agreed terms and conditions. Vendor must provide an alert service for any problems with the website hosting. This can be in the form of SMS / E-Mails and should be sent to persons mentioned in the escalation matrix.
- xxiv. The selected Vendor should backup the websites / data and should provide a failover arrangement with 15 minutes RPO and RTO with 30 minutes. In the event of main site becoming inaccessible failover arrangement should be up within 30 minutes of failure of main site. Failure cause may be site crash / hacking etc.
- xxv. Facilities should be provided by allowing remote access to Bank for websites maintenance or tuning the websites / web server. Authorized users of the Bank should be provided FTP access from dedicated IP address for periodic updating of the Websites. VPN access to the servers is also desired. Minimum 5 persons VPN access should be provided with compliance to all security norms
- xxvi. Shifting of Banks websites: Vendor must coordinate with the Bank to ensure smooth shifting of Bank's websites from the present vendor to the new hosting facility.
- xxvii. The selected Vendor should provide a minimum uptime of 99.5% availability of corporate website, calculated on a monthly basis.
- xxviii. The provided infra set up should be dedicated for Bank and no sharing of Hardware is allowed.
- xxix. The selected Vendor must configure, customize, Implement, and maintain / support the hardware / software provided and also make arrangements to provide Maintenance support, problem fixes & upgrades (Like Operating System Software problem fixes, maintenance and upgrades, MS SQL Server problem fixes, Antivirus Software problem fixes, etc.)
- xxx. The selected bidder has to close on time all audit points raised by Banks Internal or external auditors from time to time.
- xxxi. NOC & SOC services should be provided by selected vendor. If required bidder has to provide required feed to the Banks application without any additional commercial.

- xxxii. The infra provided by the selected bidder should have the provision of higher scalability, both horizontally and/or vertically. The selected vendor should also be capable of scaling the infra provided, horizontally and/or vertically, as per the Banks requirement.
- xxxiii. All the provided infra should be sized to handle the load of the Banks hosted website till the contract period.
- xxxiv. The selected bidder should ensure compliance of all Banks existing security policies and backup policies.
- xxxv. The selected bidder has to provide reports on all Database activities viz users, admin, custom access on periodical intervals prescribed by the Bank.
- xxxvi. The proposed DDoS should have a minimum features as below
  - a. **Shared Anti-DDoS services needs to be provide with all necessary security measures to be taken to protect website hacking, unauthorized access, viruses, intrusion and attacks from internal and external source/people. No separate device is required to be quoted. The selected vendor has to provide a clean internet traffic.**

**Additional Features:**

- b. Should protect ICMP attacks: ICMP floods, ping floods, smurf, IP Spoofing, LAND attack, Teardrop, IP Option Timestamp, IP Option Route Record, IP Option Source Route, Ping of Death, Tracert, ICMP Redirect, ICMP Unreachable, ICMP Large Packet.
- c. The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL handshake attack.
- d. Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Slow Connection, TCP Abnormal Connection, TCP Fragments Flood, Defence WinNuke, TCP Error Flag.
- e. Should protect UDP based attacks: UDP Flood, UDP Fragement Flood, UDP Fingerprint, Fraggles, UDP Large Packet
- f. Should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation
- g. Should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense, DNS NXDomain Defense, DNS Query Flood Defense, NS Reply Flood Defense, DNS TTL Check , DNS Source Authentication
- xxxvii. The proposed NIPS should have a minimum features as below

- a. NIPS services/functions can be combined with Firewall and all necessary security measures to be taken to protect website.**

xxxviii. The proposed Firewall should have a minimum features as below

- a. The Firewall should have a minimum 1 Gbps threat protection throughput after enabling NGFW + IPS + Antivirus+ Anti-Malware and Anti-Bot.**
- b. Features: Should support NAT64, DNS64 & DHCPv6, Traffic Shaping.
- c. The Firewall, IPSEC & SSL VPN modules shall belong to the product family which minimally attain Internet Computer Security Association (ICSA) Certification.
- d. Web Content Filtering: The proposed system should have an integrated Web Content Filtering solution without external solutions, devices, or hardware modules should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
- e. Application Control: The proposed system shall have the ability to detect, log and take action against network traffic based on over 2500 application signatures.

xxxix. The proposed WAF with ALB should have a minimum features as below

- a. The appliance should have minimum 1 Gbps of system throughput from day one and must have option to scale upto to 10 Gbps on the same Hardware
- b. Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.
- c. The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.
- d. Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies or equivalent to customize new features in addition to existing feature/functions of load balancer.
- e. Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.
- f. Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation



- g. The appliance should support Certificate format as "OpenSSL/Apache, \*.PEM", "MS IIS, \*.PFX", and "Netscape, \*.DB".
- xl. All the above network security devices should support IpV6 & IpV4 traffic.
- xli. **The vendor must take care of the below**
  - **Databases sync is required between node1 (primary/active) to node2 (secondary/passive/standby) within same Datacenter and also between active Datacenter site & standby Datacenter site**
  - **Applications (application OEM will share the details) files/folders sync is required between node1 (primary/active) to node2 (secondary/passive/standby) within same Datacenter and also between active Datacenter site & standby Datacenter site"**
- xlii. **The selected bidder has to provide the SOC1 & SOC2 certificate on yearly basis to the Bank.**

Description of the envisaged scope is enumerated as part of Annexure 12 however the Bank reserves its right to change the scope of work considering the size and variety of the requirements and the changing business conditions.

The bidder needs to quote as per the Commercial Sheet mentioned in Annexure 15

Considering the enormity of the assignment, any service which forms a part of the Project Scope that is not explicitly mentioned in scope of work as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional cost to the Bank. The Bidder needs to consider and envisage all services that would be required in the Scope and ensure the same is delivered to the Bank. The Bank will not accept any plea of the Bidder at a later date for omission of services on the pretext that the same was not explicitly mentioned in the RFP.

## **2. General Conditions**

- a) For installation & commissioning work, it shall be the responsibility of the Bidder to arrange and provide requisite tools, testing & measurement equipment and all other things required for carrying out the installation job industry practice and safety norms.
- b) The Bidder shall ensure that no other equipment / structure / setup get damaged due to their activities. Any damages caused to Bank property due to Bidder's negligence shall be passed on the Bidder's account
- c) The support shall be on 24\*7\*365 basis
- d) In the case of additional requirements desired by the Bank during the contract period over and above the quantity mentioned the maximum order which the Bank can place would be an addition of 25% of the quantity for which contract is placed.

## **3. Technical Proposal Attention Items**

- a) This RFP is not a contract offer. Receipt of a proposal neither commits Bank to award a contract to any bidder, nor limits Bank's rights to negotiate with any bidders, suppliers

or contractors in Bank's best interest. Bank reserves the right to contract with any bidder, supplier or contractor at its own discretion.

- b) Bank reserves the right to request additional information necessary and pertinent to the project so as to assure the bidder's ability and qualification to perform the contract.
- c) Failure to answer any questions within stipulated timeline at any stage of this RFP may be considered non-responsive and the proposal may be disqualified.
- d) For any ambiguity, omissions or unclear content in the RFP the bidders should request Bank to clarify along with pre-bid queries within the time line mentioned in the "[A] Important Dates.
- e) For all technical details and relevant standards and specifications of this RFP that may not be stated in detail; bidders should ensure and provide quality and industrial standard products to Bank.
- f) In case of any difference in the standards between this RFP and the bidders' proposal, the higher standards shall prevail and be applicable.
- g) Expenses incurred in the preparation of proposals in response to this RFP are the sole responsibility of the bidders.
- h) Bank reserves the right to accept or reject any and all proposals, or any part of any proposal, without penalty. Any allowance for oversight, omission, error, or mistake by the bidder made after receipt of the proposal will be at the sole discretion of Bank.
- i) Entire work specified in this RFP shall be carried out on Turnkey basis.
- j) As the contract is on Turnkey solution basis, any other miscellaneous requirements related to the scope described in the RFP or extra work required to be perform due to existing structure limitation shall be provided by the successful bidder even if those items are not mentioned explicitly in this RFP.

**Standards:** All standards to be followed will adhere to Bureau of Indian Standards (BIS) specifications or other acceptable standards.

**Service Levels and Uptime Guarantee**

For details, please refer to Annexure-13 that provides the service levels for Hosting Bank's Website (Under Opex Model in a Dedicated Infrastructure).

**4. Delivery**

The Bank expects the vendor to complete the entire job of hosting of the website including IT Infrastructure as per the requirements of this tender within 6 weeks from the date of order placement.

In case the deadlines are not met then the vendor will have to pay penalty to Bank of Baroda @ 1% of the contract value inclusive of all taxes, duties, levies etc., per week or part thereof, for late delivery of service beyond due date of delivery, to a maximum of 5%. If delay exceeds the maximum percentage of 5%, Bank of Baroda reserves the right to cancel the entire order.

Any deliverable has not been implemented or not operational on account of which the implementation is delayed, will be deemed/treated as non-delivery thereby excluding the



Bank from all payment obligations under the terms of this contract.

The bidder must strictly adhere to the delivery dates or lead times identified in their proposal and as agreed by the Bank. Failure to meet these delivery dates, unless it is due to reasons entirely attributable to the Bank, may constitute a material breach of the Bidder's performance. In the event that the Bank is forced to cancel an awarded contract (relative to this tender document) due to the Bidder's inability to meet the established delivery dates or any other reasons attributing to the bidder then that bidder will be responsible for any re-procurement costs suffered by the Bank. The liability in such an event could be limited to the differential excess amount spent by the Bank for procuring similar deliverables and services.

Incidental Services - The Bidder shall provide all the services as specified in the tender document, particularly the Project Overview and Technical Summary. The price for performing the required incidental services shall be deemed to be included in the Contract Price.

## 5. Payment Terms

The bidder must accept the payment terms proposed by the Bank. The commercial bid submitted by the bidders must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted. 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. If any of the items / activities as mentioned in the price bid is not taken up by the bank during the course of the assignment, the bank will not pay the cost of such items and professional fees quoted by the bidder in the price bid against such activity / item.

The method and conditions of payments to be made to the successful bidder shall be:

### A. Annual Rental Charges

The payment will be divided into four equal installments for the year and paid quarterly in advance, on actuals. The payment will be on production of original invoice and against receipt of satisfactory support report of previous quarter from the Bank's Project / Operation Manager.

### B. Internet Bandwidth Charges

The payment will be payable annually after end of each year against production of original invoice and against receipt of Bandwidth usage report from the Bank's Project / Operation Manager.

There shall be no escalation in the prices once the prices are fixed and agreed to by the Bank and the bidder. Payment will be released by IT Dept., as per above payment terms on submission of relevant documents.

The Bank will pay invoices within a period of 30 days from the date of receipt of undisputed invoices. Any dispute regarding the invoice will be communicated to the

selected bidder within 15 days from the date of receipt of the invoice. After the dispute is resolved, Bank shall make payment within 30 days from the date the dispute stands resolved.

## **6. Right to Alter Quantities**

The Bank reserves the right to alter the requirements specified in the Tender. The Bank also reserves the right to delete one or more items from the list of items specified in the Tender. The Bank will inform all Bidders about changes, if any. The Bidder agrees that the Bank has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities