Request for Proposal & Quote

For the Supply, Configuration & Maintenance
of
Cloud- SaaS
For

DDoS, WAF, Anti-Bot, API Security, DNS Management & CDN service Project

The South Indian Bank Ltd
Digital and Technology Department,
SIB Building, Info park Road,
Rajagiri Valley, Kakkanad,
Ernakulam – 682 039.
Kerala.

Version	1.0
Date of issue of RFPQ	06-02-2026
Type of Contract	Supply & Maintenance/subscription/Warranty Service
Purchaser Location	DC & DR
Last date for Receipt of Proposal	18-02-2026

The information contained in this RFP document, or any information provided subsequently to bidder(s) whether verbally or in documentary form by or on behalf of the Bank is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer and is only an invitation by Bank to the interested parties for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist the formulation of their proposals. While effort has been made to include all information and requirements of the Bank with respect to the solution requested, this RFP does not claim to include all the information each bidder may require. Each bidder should conduct its own investigation and analysis and should check the accuracy, reliability and completeness of the information in this RFP and wherever necessary obtain independent advice. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. The Bank may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

Table of contents

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

1. ABOUT OUR BANK

The South Indian Bank Limited (website-www.southindianbank.bank.in) is one of the leading Scheduled Commercial Bank having more than 948 branches & 1143 ATMs spread across 30 States & Union Territories in India. The Head (Registered) Office of the Bank is situated at Thrissur, Kerala State. There are Nineteen Regional Offices (ROs), geographically spread across the country, coming under the administrative control of the Head Office.

The South Indian Bank Limited offers various customer services such as Anywhere-Any Time Banking supported with online ATMs, Internet Banking, International ATM-Cum-Debit Cards, Mobile Banking, online payment, online trading etc. The Bank has already adopted significant technological advancements and uses them to leverage business operations such as NDS-PDO, RTGS, NEFT, Domestic ATM sharing, NPS, SWIFT, Treasury, Forex, POS, etc.

Bank has been awarded with ISO 27001:2013 Certification for Information Security Management Systems (ISMS).

2. OBJECTIVE

Objective of this RFPQ is to undertake tendering (separate technical & commercial) for empanelment of vendors for the purchase of new DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solutions that will enhance our organization's network security infrastructure. Bidders who are interested in participating in the RFPQ must fulfill the eligibility criteria mentioned in the document.

3. TERMS & ABBREVIATIONS USED IN THIS DOCUMENT

1) **'Bid'** shall mean the set of Bid/Request for Proposal and Quote (RFPQ) documents provided by Vendor to the bank for submitting a competitive quotation for the execution of 'Works' in accordance with the terms specified in this document.
2) **'SIB/Bank'** means The South Indian Bank Ltd.
3) **'Vendor/Provider'** means the entity who has submitted the Bid documents for the said ''Works' with the intention of submitting a competitive quotation for the execution of Works in accordance with terms specified in this document.
4) **'Service Level Agreement'** shall mean the Contract entered between Bank and the successful Vendor on award of Contract for Works.
5) **'Successful Vendor'** means the Vendor whose Bid is accepted by the Bank and been awarded the Contract of Works.
6) **'CBS'** – Finacle Core banking solution installed at our Data Center.
7) **'RFPQ'** – This Request for Proposal & Quote
8) **'Full Acceptance'** means the solution has been 'fully implemented' and has passed the acceptance test as per the acceptance test plan.

4. PROJECT OVERVIEW AND SCOPE OF WORK

This RFP document has been prepared solely for the purpose of enabling SIB to select a bidder for the supply, configuration and maintenance of DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution at DC & DR for a period of 5 years.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

SIB intend to procure DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution with 5-year subscription/warranty/support as a replacement of existing WAF used in our network on account of its End-of-Support-Life (EoSL)

The bidder's scope of work also following activities and deliverables but not limited to:

1) The bidder shall supply **of DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution with Total 5-year warranty/support/subscription cost**. However, the Bank will place order for DDoS, WAF, Anti-Bot, CDN service & API Security Solution as per Bank's requirement. The payment for the mentioned services may yearly basis and SIB have the power to terminate the services from SI/OEM as per bank's decision.
2) Bidder shall be responsible for the supply of all necessary hardware and software products, if any required onsite for achieving any of the functionalities mentioned in the RFPQ. Also, Configuration and Integration of applications with existing network at DC and DR. All latest stable hot fix should be applied on DDoS, WAF, Anti-Bot, CDN service & API Security Solution.
3) The bidder must provide On-site, comprehensive BACK-TO-BACK Warranty/support/subscription from OEM for a period of 5 years from the date of acceptance.
4) The warranty/support/subscription also includes all software subscriptions (critical hot fixes, service packs, and all upgrades/updates) of all components supplied as part of solution.
5) The bidder has to ensure support (24x7 with 30 minutes response) as and when required for resolving all DDoS, WAF, Anti-Bot, CDN service & API Security Solution related issues and other required features procured in this RFP, during warranty/support/subscription and ATS (Annual Technical Support) period (or such other extended period as per the contract terms and paid maintenance will commence only thereafter).
6) The DDoS, WAF, Anti-Bot, CDN service & API Security Solution quotes should be from a reputed OEM having previous experience in Configuration/installation and, OEM professional services need to be provided for the deployment. OEM can submit only one proposal either directly or through any of the preferred partner.
7) The hardware if any, supplied as part of this contract should be the latest box and not be declared End of Sale for period of 5 years from last date of submission of bids and should not be End of support for at least 5 years from thereon.
8) The bidder must be a premium business partner with an authority to sell, upgrade, supply, service and maintain the product positioned and a letter of authority to this effect must be accompanied with the response.
9) The Bank may, during the currency of the warranty, shift the equipment if any, supplied as part of this contract to other location(s) within the Country. The bidder needs to ensure that the OEMs and bidders' warranty and support is valid across India. Further, bidder undertakes to continue to provide warranty and support the goods at the new location.

5. TECHNICAL REQUIREMENTS

The Bank is preferably considering Services from the market leading OEM/Vendors. Vendor is requested to submit the checklist/supporting documents for all the functionalities described in Annexure I along with the response.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

6. TRAINING

1) The Bidder shall arrange the certified training program from OEM for at least six officials of Bank.
2) Training should be of OEM certification level standard with certified training materials.

7. SERVICE LEVEL

This section describes the service levels that have been established for the Services offered by Vendor to the Bank. Vendor shall maintain the stated service levels to provide quality customer service to the Bank.

1) The bidder has to ensure support (24x7 with 30 minutes response) as and when required for resolving all DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution related issues and other required features procured in this RFP, during warranty/subscription and ATS (Annual Technical Support) period (or such other extended period as per the contract terms and paid maintenance will commence only thereafter).Response should be onsite.
2) The vendor must offer onsite comprehensive support (premium OEM support) to the DDoS, WAF, Anti-Bot, DNS,CDN service & API Security Solution includes hardware (if any) with initial response from vendor and all the related components for a period of **five years** from the date of fully delivered to the Bank.
3) Products positioned must have a roadmap and life span of minimum 5 years. The Vendor shall not quote any product that is End of Life or due for End of Life in the next 5 years. If any of the devices/service (if any) is being declared as End of life during the contract period, it should be replaced by the equivalent or higher version without any conditional cost to the bank.
4) Penalty Computation: In the event of Service Level Default, Bank will charge a penalty of 18% per annum on the total purchase order value for the delayed number of hours for major complaints minor complaints
    a. Incident Acknowledgment*:* ≤ 15 minutes for critical security incidents; ≤ 30 minutes for high severity; ≤ 1 business day for non-critical issues.
    b. Automated Mitigation*:* The platform must initiate automated attack mitigation in real time upon detection.
    c. Resolution Targets*:* Major issues (service outage/DDoS mitigation issues) resolved or effectively mitigated within 1 hours; less severe issues resolved within 1 business day

8. SUPPLY, DELIVERY AND ACCEPTANCE

The selected vendor will be adhered to the Time duration and acceptance test as follows

1) **Delivery:** The selected vendor shall be responsible for delivery of the ordered item(s) at the bank's specified location at no extra charge within 3-4 weeks from the date of purchase order.
    a. The Road Permit and other necessary documents are to be arranged by the vendor within delivery period of without any additional cost to Bank.
    b. Appropriate insurance to cover the ordered item(s) for the transit period and till the time of its acceptance by the Bank at the respective site is to be take care by the vendor. The cost of the insurance will be borne by the Bidder.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

c. If delivery is delayed, bank will charge a penalty of 18% per annum of order value for every day of delay, subject to a maximum of 10% of the order value or will lead to cancellation of the purchase order itself. However, the Vendor shall make all endeavors to deliver all items before the date.

d. The support period for the supplied equipment (if any) (including software and hardware provided by the Bidder pursuant to this Agreement) will commence after 100% delivery.

2) **Supply:** The Digital and Technology Department is floating this RFPQ. However, the Bidder(s) getting the contracts shall deliver, and operationalize the equipment, procured through this RFPQ, at the Bank's locations or at such centers as the Bank may deem fit and the changes, if any, in the locations will be intimated to the Bidder.

   a. Bidder should ensure that the DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution and its associated components (if any) delivered to the Bank including all components and attachments are brand new. In case of software supplied with the system, the Bidder should ensure that the same is licensed and legally obtained with valid documentation made available to the Bank.

3) Acceptance: The delivered appliance (if any) should be manufactured post the PO date.

4) PoC Testing: The Original Equipment Manufacturer/service provider/System Integrator should be ready to do POC at no cost and no obligations to SIB. All necessary service/equipment & software should be supplied by vendor for POC of DDoS, WAF, Anti-Bot, CDN service & API Security Solution. If vendor/OEM is not ready to carry out POC as per the terms, Bank reserves the right to reject the proposal.

9. TERMS & CONDITIONS

1) SIB reserves the right to either not to implement the service/devices/solution or to partially implement the service/devices/solution.
2) SIB reserves the right to split the orders for different products among the quoting vendors.
3) SIB reserves the right to open the quotations soon after their receipt from all the vendors without waiting till the last date specified.
4) Bid should strictly conform to the specifications. Bids not conforming to the specifications will be rejected summarily.
5) Any incomplete or ambiguous terms/ conditions/ quotes will disqualify the offer.
6) Any set of terms and conditions from the Vendors are not acceptable to the Bank.
7) The Bank reserves the right to cancel the contract placed on the select vendor if the Vendor commits a breach of any of the terms and conditions of the bid Vendor goes into liquidation voluntarily or otherwise Progress made by the selected vendor is found to be unsatisfactory.
8) SIB reserves the right to accept or reject any bids without assigning any reason thereof and SIB's decision in this regard is final.
9) The Bank reserves the right to stop the RFPQ process at any stage and go in for fresh RFPQ without assigning any reasons or to modify the requirements in RFPQ during the process of evaluation at any time.
10) SIB is not responsible for non-receipt of quotations within the specified date and time due to any reason including postal holidays, delays or approaching SIB.
11) Any response to the RFPQ that do not meet the set timelines or incomplete in any aspect, will be summarily rejected at the whole discretion of the bank.
12) SIB is not bound to place on the order on the lowest price Vendor or the best technical Vendor.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

13) The Bank reserves the right to order individual service/items, if required at the prices quoted by the vendor(s).
14) SIB reserves the right to re-negotiate the prices in the event of change in the market prices/situations of both the service/hardware and software.
15) SIB reserves right to call for a post bid meeting for clarifying its queries at the banks premises.
16) In case the selected vendor fails to deliver the items of hardware/software, and all other related peripherals stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the selected vendor.
17) SIB reserves the right to cancel the Purchase Order if the items are not delivered within the agreed period from the date of purchase order unless extended in writing by SIB.
18) SIB can disqualify any Vendor who fails to sign the Service Level Agreement with bank.
19) The vendor shall keep the offer valid for one calendar month from the last date of submission of RFPQ.
20) SIB is very much interested in long-term association with the potential Vendor and hence Vendor shall adapt to changes in SIB requirements and provide superior Products and Services and not by mere fulfillment of contractual commitments set here forth.
21) All inquiries, communications and requests for clarification shall be submitted in hard copies/e-mail to SIB and response for the same shall be obtained in writing. Only such documents shall be considered as authoritative.
22) All intellectual property related to the project shall be the property of SIB and SIB reserves the right from its sole discretion to implement the same at other centers in future with/without involving successful Vendor.
23) Product/service should be free from known bugs at the time of supply.
24) Product/service should be able to comply with network baseline requirements.
25) Technical discussion will be held directly with OEM/service provider, if more than one bidder partners with same OEM/service provider. OEM/service provider will communicate with the bidder about the technical discussion post completion of the same.
26) If Bank is not satisfied with the Price Discovery in this process, bank reserves the right to initiate the tendering process again through Limited or Open tender for any Equipment which is part of the scope of work.

10. VENDOR RESPONSIBILITIES

1) Vendors shall share its technology strategies, direction, and product path and research & development efforts with SIB.
2) Vendors shall adhere to the procedure and processes laid down in this document.
3) Vendors shall alert SIB and its own personnel about the risks either anticipated or faced either prior and/ or during and / or after the execution of the project and provide all the possible solutions either to totally eliminate or to minimize such risks.
4) Vendors shall extend all the services and ensure that SIB benefit on the basis of Most Favored Customer Pricing Mechanism.
5) Vendors shall ensure all possible efforts in continuous improvement in processes, tools and procedures and practice the world-class methodologies in delivering Products and Services.
6) Successful Vendor shall protect and fully indemnify the SIB from any claims for infringement of patents, copyright, trademark or the like.
7) Vendor shall not sub-contract all or any part of the scope of proposal or any other services which includes maintenance etc., to any 3rd party. Any services which need to be rendered to Bank should be done by on-roll employee of the Vendor organization.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

8) Vendor shall provide the escalation matrix & centralized help desk number for call logging to the Bank.
9) The vendor shall explicitly absolve the Bank of any responsibility/ liability for the use of system software, with regard to copyright/ license violations, if any.
10) Vendor should ensure that all points in the RFPQ document are taken into account before submitting the Bid Documents.
11) If any particular point mentioned in the RFPQ are not able to adhere by the vendor should mention separately along with the proposal.
12) Vendor should provide the list of banks/financial institutions/corporates in India to which they are currently offered and delivered the proposed product/solutions.
13) Vendor shall provide all the latest upgrades released by OEM on time-to-time basis, for all the devices without any extra cost to the Bank during the period of Contract.
14) The Vendor's representative is the contact point for the Bank. The delivery status of service/equipment should be reported on a weekly basis.

11. LITIGATION

1) The bidder shall indemnify the Bank and be liable for any loss due to malfunctioning of the devices and all its related components under the project as it is supplied and installed by them.
2) If it comes to the notice of the Bank that the Vendor has suppressed any information either intentionally or otherwise, or furnished misleading or inaccurate information, the Bank reserves the right to disqualify the Vendor. If such information comes to the knowledge of the Bank after the award of work, SIB reserves the right to terminate the Contract unilaterally at the total cost and risk of the Vendor. The Bank also reserves the right to recover any dues payable by the selected vendor from any amount outstanding to the credit of the selected bidder, including the pending bills etc., if any. The Bank will also reserve the right to recover any Advance paid.
3) Work under the Contract shall be continued by the selected vendor during the arbitration proceedings unless otherwise directed in writing by the Bank unless the matter is such that the works cannot possibly be continued until the decision of the arbitrator or of the umpire, as the case may be, is obtained and save as those which are otherwise explicitly provided in the Contract, no payment due or payable by the Bank, to the vendor shall be withheld on account of the ongoing arbitration proceedings, if any, unless it is the subject matter or one of the subject matter thereof. The venue of the arbitration shall be at Thrissur, Kerala State, India.

12. SELECTION CRITERIA

1) The Vendor is expected to submit the proposal with favorable and competitive price and service capabilities. SIB will select the Vendor, product/solution, which it believes offers the proposal, which is in SIB's best overall interest. SIB will select proposals with which to negotiate and reserves the right to enter into a contract with a Vendor that may not be lowest in fees charged. In determining the successful Vendor, SIB will consider, but not be limited to, the following selection criteria:
    a. **Ability to Execute→** Implementation Methodology, Client Feedback, History of product migration/ upgrades.
    b. **Service and Support→** Implementation Planning, Implementation, Migration, and Post Implementation/ Migration.
    c. **Costs→** All-Inclusive Costs.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

d. **Functionality→** Delivered Functionality, Interface Capabilities and Training capabilities
e. **Technology→** Architecture, Process for Modifications or Customization, Operational Impact, and Toolset
f. **Vendor's Vision→** Short- and long-term goals, Development Philosophy, and Track Record for Implementing Past Vision, Financial Stability.
g. **Deployment of proposed devices→**Whether the vendor has deployed the proposed version of the equipment's/hardware/software in any Bank/financial institution/data center in India.

13. COMMERCIALS

1) The Bidder is requested to quote in Indian Rupees ('INR'). Bid in currencies other than INR will be rejected and Bidder will be disqualified. The prices quoted for the HLBs in the commercial bid should be valid during the warranty period.
2) In case of there is decrease in the prices of the DNS Management, DDoS,WAF,Bot,CDN service & API Security Solution's during the tenure of the contract; the cost benefit should be passed to the bank.
3) The prices should be exclusive of GST. The price should be inclusive of other charges, as applicable, like excise, custom duties, packing/ forwarding/ freight/ transit insurance, etc., A clear price break-up should be indicated for all the components supplied/installed.
4) The prices quoted by the vendor shall be in Indian Rupees, firm and not subject to any price escalation. All payments made will also be in Indian Rupees only.
5) All the associated hardware/software/third party tools etc required if any for implementation, should be clearly given in the commercial offer.
6) Further, after the orders being placed/agreement executed, the Vendor shall pass on to bank all fiscal benefits arising out of reductions in Government levies viz. sales tax, excise duty, custom duty, etc.

14. TERMS OF PAYMENT

Following will be the terms of Payment for the Hardware and other infrastructure supplied.

1) The payment milestones are as follows:

Payment	Milestone
10%	After the complete acceptance of the Purchase Order and the Initial discussion of Implementation plan.
40%	Shall be payable upon successful tenant/ service creation for DNS Management, DDoS, WAF, Anti-Bot, CDN service & API Security Solution. Completion of initial configuration and integration documentation.
40%	Payment shall be processed only after successful completion of the integration and migration of all existing applications (web/mobile) to the proposed solution, subject to the acceptance by the bank.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

10%	After submission of complete documentation, completion of relevant training and signing of SLA & NDA and submission of Performance Bank Guarantee valid for three years for 15% of total order value.

2) Payments will be made only on submission of invoice and other documents necessary as per the terms agreed upon.

15. AMENDMENT TO RFPQ

The Bank also reserves the right to change any terms and conditions of the RFPQ and its subsequent addendums as it deems necessary at its sole discretion. The bank will inform the Bidder about changes, if any before the commercial bids are opened.

1) The Bank may revise any part of the RFPQ, by providing an addendum to the Bidder at any stage till commercial bids are opened. The Bank reserves the right to extend the dates for submission of responses to this document.
2) Bidder shall have the opportunity to clarify doubts pertaining to the RFPQ in order to clarify any issues they may have, prior to finalizing their responses. Responses to inquiries and any other corrections and amendments will be distributed to the Bidder in electronic mail format or hardcopy letter or at Bank's website, at the sole discretion of the Bank.
3) Preliminary Scrutiny – The Bank will study the offer to determine whether it is complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. The Bank may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on the Bidder, and the Bank reserves the right for such waivers and the Bank's decision in the matter will be final.
4) Clarification of offer – To assist in the study, evaluation and comparison of offer, the Bank may, at its discretion, ask the Bidder for clarification of their offer. The Bank has the right to disqualify the Bidder whose clarification is found not suitable to the proposed project.
5) 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 or increase one or more items from the list of items specified in the tender. The bank will inform the Bidder about changes, if any. In the event of any alteration in the quantities the price quoted by the Bidder against the item would be considered for such alteration. The Bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by Bank for alteration in quantities. Bidder agrees that there is no limit on the quantities that can be altered under this contract.

16. RESPONSE TO RFPQ AND CONTACT DETAILS

The time is the essence of the project. It is mandatory for vendors who respond to this RFP to meet these expectations as they are tightly linked to SIB's plans of offering quality services to its customers at the earliest. Following are the timeframe defined for the activities.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

ACTIVITY	DATE
Address any clarifications on RFPQ (Clarifications may be addressed by e-Mail and can be obtained by sending a mail to→ dtdinfosec@sib.co.in with subject line ***"RFPQ FOR DNS management,DDoS,WAF,Anti-Bot,CDN service & API Security Solution"***)	16-02-2026
Bid submission-Last Date	18-02-2026

However, the Bank reserves the right to extend the last date of submission, at its sole discretion.

1) Bidders are required to direct all communications for any clarification related to this RFPQ, to the Designated Bank officials. All queries relating to the RFPQ, technical or otherwise, must be in writing only i.e. either via physical or electronic mail. The Bank will try to reply, without any obligation in respect thereof, every reasonable query raised by the Bidder in the manner specified.
2) Response to the RFPQ should be submitted in a single bid. The commercial bid should include only the commercials; all other information (including the Mandatory Response Sheet and all documents/materials mentioned in the same) should be included in the Technical Bid.
3) Vendors should submit bids in sealed covers. Each bid should be submitted in two sets (i.e. in hardcopy and softcopy) duly sealed
4) Bids with erasure / overwriting / cutting are liable to be rejected. If required, the corrections can be made by scoring out and writing afresh. The corrections shall be authenticated with authorized signature.
5) Bids once submitted shall be final and no amendment shall be permitted. A Vendor shall submit only one set of proposals and aligned with single OEM. The vendor should certify that the contents of the CD's are the same as that provided by way of hard copy. In the event of a discrepancy the offer will be rejected.
6) Vendor should ensure that the bid document reaches the following address on or before to:

Assistant General Manager - InfoSec
Digital and Technology Department
The South Indian Bank Ltd
DTD-INFOSEC, SIB Building (1ST Floor), Infopark Road
Rajagiri Valley, Kakkanad
Ernakulam – 682 039, Kerala State
E-mail: dtdinfosec@sib.co.in
Mobile:9446375056

7) The South Indian Bank Limited reserves the right to accept or reject any or all the bids without assigning any reason whatsoever. Any decision of The South Indian Bank Limited in this regard shall be final, conclusive and binding on the bidder.

17. Termination

Termination for Default: The Bank, without prejudice to any other remedy for breach of contract, by written notice of default sent to the successful vendor, may terminate this contract in whole or in part:

1) If the Successful Vendor fails to perform obligation(s) under the contract.
2) If the Successful Vendor, in the judgment of the Bank has engaged in corrupt or fraudulent practices in competing for or in executing the Contract. Corrupt practice means the offering, giving, receiving or soliciting of anything of value or influence the action of an official in the bank in procurement process or in contract execution; and "fraudulent practice" means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of the Bank, and includes collusive practice among Vendors (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.

Apart from the general grounds of default mentioned above, the Bank reserves its right to cancel the order in the event of, but not limited to, one or more of the following specific situations:

3) Unnecessary or unwarranted delay in execution of the work allotted.
4) Delay in submission of reports beyond the stipulated periods.
5) Breach of trust is noticed during any stage of the consultancy assignment.
6) The selected Vendor commits a breach of any of the terms and conditions of the bid.
7) If it is found at any stage that the Vendor has concealed any important information or has submitted any false information or declaration particularly regarding any pending legal action or blacklisting status.

18. MANDATORY RESPONSE SHEET

This is a Mandatory response expected from the Vendor, bidding for the RFPQ of South Indian Bank Ltd. Kindly provide appropriate response to the particulars asked for:

No	Particulars	Your Response
Contact Details(Solution Provider/OEM)		
1	Name of Solution Provider/OEM	
2	Postal Address	
3	e-mail	
4	Phone	
6	Contact Person	
7	Contact Person Designation	
8	Date of Incorporation	
Contact Details(Implementation Partner)		
1	Name of Implementation Partner	
2	Postal Address	
3	e-mail	
4	Phone	
5	Fax	
6	Contact Person	
7	Contact Person Designation	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

19. FUNCTIONALITY/ TECHNICAL RESPONSE DOCUMENT

Vendor is requested to reproduce all the points in the annexure and furnish the appropriate response to the particulars asked by giving the compliance level as explained below. Explanations/suggestions for each point can be provided in a Remarks column.

Compliance	Description
YES	Already Available FULLY in the product.
NO	Not Feasible in the product due to architecture or structural limitations.

20. Commercial Bid Details

Sl	Particulars	DC	DR	Total
1	*Cloud tenant for DNS, DDoS, WAF, Anti-Bot,CDN service & API Security Solution	Both		1
2	**API Security solution ancillary components (IF ANY)	1	1	2
3	**Custom Configuration/ OS for any product specific configuration (IF ANY) required as part of accomplishing technical requirements in the Annexures. Example: On prem VM configuration and custom configuration deployments			
4	Implementation cost -One time			
5	*Support Cost			
6	Training cost -One time			

The bidder/OEM shall provide pricing for a five-year subscription term. Payment shall be made by the bank annually in accordance with the criteria defined in the RFPQ.

*** Should be quoted Top business model for the product/support**

****The bidder/OEM shall explicitly propose and detail any additional on-premises infrastructure components, wherever required, to meet the stated business requirements, application integration needs, or regulatory/compliance obligations, in cases where the proposed cloud-based solution is not capable of fully complying with the RFP requirements.**

Notes:→

a. Price must be in Indian Rupees.
b. Wherever license/subscriptions are involved, it must be unambiguously mentioned.
c. The cost must be exclusive of taxes and separate tax % prevailing at the time of quote may be mentioned.
d. Based on the technical evaluation and final commercials, PO shall be issued to a Single Vendor.
e. Quote must be firm for a minimum of 30 days from date of closure of bid.

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

21. Annexures

Annexure 1 : Technical requirements

Sl	**Area of Consideration – Cloud DNS, DDoS, WAF/WAAP,Bot, CDN, API security Solution**	Compliance-Yes/NO Remarks, if any
1	The proposed solution must support fully cloud based Authoritative DNS solution providing low latency, reliable and secure DNS communication and DNS Platform should offer 100% Availability SLA	
2	DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have N number of POPs globally with multiple POPs in India as well.	
3	DNS solution should support dedicated static Indian IPs (IPV4 & V6) for authoritative name servers and provide direct authoritative responses to recursive DNS servers when asked about the domains managed through the solution. The authoritative name server host name should be customizable as per Bank's requirement in the format supported by registrar	
4	The solution should provide separate unique Name server Ips for each primary domain/zone configured in solution	
5	Solution can add DNSSEC feature for the domain/ subdomain wherever required and should be able to support DNS cache poisoning prevention.	
6	Solution can do DNS Management (A record, TXT record, CNAME, etc) for the domain/subdomains wherever required	
7	The solution must provide a management console (GUI) for managing DNS records also provide API for creating, modifying, and deleting DNS records	
8	The solution must enforce Two Factor Authentication for registered users and Role Based Access Control (RBAC)	
9	Solution should support both primary and secondary DNS deployments	
10	OEM should provide Always on DDOS security solution with proven DDOS defines capacity of more than 10Tbps.	
11	OEM Infrastructure should have multiple scrubbing centres (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	
12	The solution shall support application-wise bandwidth shaping and traffic throttling, particularly during events such as bot attacks, abnormal traffic surges, or denial-of-service–like conditions, to ensure service availability and optimal performance.	
13	The Proposed solution should support inspection of ipv4 and ipv6 attacks.	
14	The proposed solution should be able to block traffic based on Geo location, Range of IP's, Specific Ip's	
15	The proposed solution should support integration of third-party external Threat Intelligence Platform.	
16	Solution should provide real time Detection and protection from unknown Network DDOS attacks. The methods for detecting DDoS attacks, should include signature-based detection, anomaly detection, and behavioural analysis.	
17	System should Protect from Brute Force/reflection & DNS amplification attacks or equivalent.	
18	The proposed Solution should support for all protocols at layer 3 to layer 7 and able to detect and block all type of Flood attacks.	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

19	Cloud DNS, CDN,DDOS, WAAP/WAF, Api Security solution should integrate with existing SIEM engine seamlessly through syslog and shall provide APIs to retrieve security event data from the cloud service on a near real-time basis	
20	The proposed solution shall provide centralized management for administration, reporting, detection, and mitigation across all WAF instances from a single management console. And capable of generating periodic reports, real-time and historical GUI-based reports for a minimum period of six (6) months and custom / pre-defined graphical reports, both on demand and on a scheduled basis which can be emailed or downloaded from the centralized management console • Attack types • Source and destination IP addresses • Blocked hosts • Top targeted URLs	
21	The proposed WAF solution should support positive, negative and hybrid security models to support inspection of traffic passing through WAF	
22	Cloud WAF platform shall comply with relevant certifications such as SOC 2 Type II, ISO 27001, and PCI DSS.	
23	Cloud WAF solution shall comply with RBI data localization requirements, ensuring that all logs and metadata are stored and processed within India	
24	Encryption keys shall be customer-managed (preferred).	
25	The proposed Cloud WAF solution shall forward traffic securely to the Bank's Data Centre or application origin.	
26	The solution shall support log retention (management events, security alerts, etc.) for a minimum period of one (1) year.	
27	The solution shall support masking of sensitive data in alerts and reports.	
28	The solution shall support cryptographic agility to enable future adoption of Post-Quantum Cryptography (PQC) in line with RBI, NIST, and global standards.	
29	In a hybrid deployment model, no sensitive data shall be transmitted from the Bank's internal Data Centre or private cloud environment to any cloud-based infrastructure, including the Cloud WAF platform	
30	The proposed solution shall fully comply with the Digital Personal Data Protection (DPDP) Act, 2023. The vendor shall act as a Data Processor, processing personal data solely on documented instructions from the Bank, which acts as the Data Fiduciary, and only for the purposes of providing the contracted services.	
31	The proposed WAF solution should support following inspection criteria Signature Matching IP address filtering Geolocation Blocking Rate Limiting Protocol validations Behavioural analysis and Anomaly detection Http content inspection Bot Management	
32	When a WAF rule is triggered, it should support following actions Block/Allow/Log/Challenge. IP whitelisting and blacklisting etc.	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

33	shall include an IP reputation engine with a dedicated dashboard to view and evaluate the risk score of IP addresses, enabling enhanced threat visibility and seamless integration with SOAR platforms.	
34	Cloud service providers should not have any restrictions on the amount of throughput or SSL transactions it can serve and should offer scalable capacity on Demand	
35	The SSL encryption/decryption process in WAF should not create any privacy concerns and it should be fully complied with regulatory directions	
36	The proposed solutions should support secured SSL certificate and key management functionalities. Some of the existing web applications in our Bank uses mTLS and SSL pinning features. The solution should have capability to integrate and protect such applications without any application-level changes and all application-level functionalities should work as expected.	
37	The proposed solution should support all existing and evolving cryptographic standards	
38	Some of the existing web applications are using custom ports (other than 80 & 443) for application access, the proposed solution should support this feature. Since IP whitelisting is mandatory for integration with government agencies, the proposed solutions should provide static Ips to host application domains.	
39	Should provide service of presenting a static/alternate version of the site in case if origin server is not available OR the customer can specify content to be served out of cache on the CDN in the event of an origin failure OR failover to alternate data centre – if the customer has more than one origin server	
40	The high availability of the services shall not entail performance degradation while delivering the CDN services and will not negatively affect the origin.	
41	Caching of content with configurable 'Time to Live (TTL)' values along with Caching of static content like JS, CSS, Images on cloud platform	
42	The solution shall support caching (for non-sensitive static content only), compression of web content, and SSL acceleration.	
43	Cloud Service Provider should provide following reports - Hits by Geography (Country wise) - Top URLs - Route Optimization, In percentage of accelerated requests - Hits Offload - Volume Offload - Hits by Response Type - HttP consumed Data etc	
44	Cloud based WAF should provide protection against following Application Layer attacks directed at Hostnames on all application ports exposed - Generic Attacks - SQL Injection - Cross Site Scripting - Command Injection - Directory Indexing - Cross Site Scripting signature - Invalid HTTP - Remote File Inclusion - PHP Injection - Trojan Backdoors	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

	- DDoS - Path Traversal Attack - Protocol Violation - Information leakage	
45	Cloud based WAF should be able to provide protection against following Network/Distributed Denial of Service Attacks directed at Hostnames on all application ports exposed - UDP Fragments - ICMP Floods - SYN Floods - ACK Floods - RESET Floods - UDP Floods - GET Floods - HTTP slow client (“drip feed”) DDoS attacks like Slow Loris	
46	Cloud based WAF should be able to provide following Network-Layer Controls - Ability to enforce customer-defined IP whitelists and blacklists - Ability to enforce list types based on ASNs or TLS fingerprints - Able to provide Classless Inter-Domain Routing (CIDR) lists - Able to block or mitigate The Onion Router (Tor) traffic - Geo-blocking	
47	Cloud based WAF should be able to provide following Rate Polices - Security Service Configuration should allow Rate Control Policies with configurable Bursting Threshold and Average Threshold - Rate control polices can be applied in a granular fashion by applying match criteria: o User-based rate limiting o Source IP–based rate limiting o Connection-based limits o Session-based limits o ASN level Other relevant traffic control scenarios	
48	WAF service shall scale automatically, on-demand, offering the capability to defend against massive-scale attacks with no-cap on the size of attacks. In these scenarios’ s WAF shall inspect both HTTP and HTTPS requests.	
49	The solution shall be capable of validating encoded data within HTTP traffic.	
50	The solution shall identify WebSocket and WebSocket Secure (WSS) connections and provide security controls against: o Server abuse o Authentication bypass o XSS and SQL injection attacks (where payload inspection is supported)	
51	The Web Application Firewall shall provide Anti-Automation protection to block automated attacks executed using hacking tools, scripts, and frameworks	
52	The solution shall include mechanisms to detect/block brute-force attack	
53	The solution shall support creation of base security policies with inheritance to child policies. Inheritance shall support restricting modifications to base policy settings.	
54	The solution shall allow administrators to add, modify, and fine-tune signatures.	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

55	The proposed solution shall be capable of automatically detecting backend software technologies to recommend appropriate signature sets for the defined security policy	
56	The proposed solution shall support configuration of custom request payload analysis rules on a per-URL basis	
57	The solution shall be capable of logging full session metadata, subject to masking of sensitive fields, when suspicious transactions are detected	
58	The solution may support user-written scripts to control application flows, subject to Bank security approval	
59	Behaviour-Based Traffic Management: The solution shall support advanced, granular, and context-aware traffic control mechanisms beyond traditional IP-, geo-, or static rule–based controls. This shall include, but not be limited to: - Behavioural analysis based on request patterns, frequency, anomalies, and reputation - Adaptive rate limiting based on user/session/API behaviour - Risk-based enforcement using contextual attributes such as device fingerprint, user behaviour, request velocity, and historical trends - Dynamic policy enforcement to distinguish legitimate traffic surges from malicious or automated activities	
60	Solution should provide SSL/TLS options (Universal SSL, advanced certificate, custom certificate, origin certificate) & ability to custom TLS communication with cipher suites	
61	Virtual Patching & Zero-Day Protection: The solution must support virtual patching capabilities to mitigate zero-day and newly disclosed vulnerabilities, without requiring immediate application code changes or downtime, until permanent remediation is applied at the application or infrastructure layer.	
62	SIB's internet banking application uses a unique client-authentication mechanism like mTLS. When users access the application, authentication is initiated using a CA-validated DSC (Digital Signature Certificate), and the corresponding CA details are registered with the 2FA server, Snorkel. The client machine connecting to the web server must present a user certificate that is already registered with Snorkel. The proposed solution should be capable of supporting this type of certificate-based authentication mechanism.	
63	The solution shall support detection and prevention of malicious uploads and payloads using both behavioral and signature-based analysis.	
64	When traffic is proxied, the origin server shall receive the original client IP address via a standard forwarded header (e.g., X-Forwarded-For); this is required for proper security enforcement and logging	
65	DDoS controls should adapt dynamically to evolving attack techniques without relying on predefined rules	
66	Real-time Bot Visibility & Analysis: The service shall provide real-time visibility into security data, including bot activity across all customer-facing web applications. It shall identify and categorize automated bot traffic, offering detailed insights—such as bot types, volume, hits, page views, and bandwidth consumption—through an integrated visualization and reporting interface.	
67	Advanced Bot Mitigation & In-line Protection: The in-line, distributed service shall ensure optimal application performance while preventing advanced threats by enforcing bot-management actions at the provider infrastructure before traffic reaches the origin. The solution shall also support creating custom bot-mitigation rules based on bot scores and other relevant attributes.	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

68	Breakdown of bot traffic by: - Bot Category - IP address - IP subnet - Country - URL - ASN - hostname - action applied. - http response code - security policies & - Botnet identifier	
69	Security Dashboards should have Reports for Bots, Client reputation, Security trends, DDOS Trends & more.	
70	Anti-BOT Solution should have SDK to support Android and iOS Apps. SDK should be able to retrieve user telemetry and send it to Bot Solution for verification.	
71	The Anti-Bot solution must use advanced AI/ML based detection and research capabilities to identify, classify, and mitigate malicious bot traffic in real time, while continuously adapting to new and evolving bot behaviours with minimal false positives.	
72	Anti-BOT Solution should not be disjointed, or 3rd party. It should be integrated & available via same platform such as CDN, WAAP along with Advanced Bot Solution. All of them should work inline.	
73	Advance Web Scraping Anti-BOT Solution should stop persistent scrapers from stealing content that can be used for malicious purposes.	
74	Solution should provide High-Level categories of BOTs: Solution Provider BOT Categories, Customer Defined BOT Category, and Unknown BOTs Category.	
75	Solution shall be able to automatically apply mitigation features, like, rate limiting when anomalous attack patterns are detected.	
76	The solution shall address and mitigate the OWASP Top 10 Web Application and Mobile Application Security Vulnerabilities (latest published version).	
77	The solution shall provide an OWASP Dashboard with a holistic and interactive interface that: o Maps application risks and protections against OWASP Top 10 categories o Displays the application's security posture o Provides recommendations to address identified gaps o Allows configuration of relevant security policies	
78	The solution shall provide a centralized API Inventory and Discovery Dashboard with the capability to automatically and continuously discover all APIs across the environment. The dashboard must display, at a minimum: - Complete inventory of all detected APIs, including known, shadow, and zombie APIs - API versioning details (e.g., v1, v2, v3) - Classification of APIs as internal or external - Identification and tagging of sensitive endpoints, including but not limited to authentication, account balance, payment, and transaction APIs - Risk score per API based on configurable security parameters - Visibility into newly discovered APIs with discovery timestamp	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

	- API performance metrics, including Average latency, p95 latency, p99 latency	
79	The solution shall provide a real-time API Security Threat Dashboard capable of detecting, classifying, and visualizing API-specific attacks. The solution must detect and report the following threats, at a minimum: - OWASP API Top 10 violations with compliance mapping - Authentication and authorization failures - Broken Object Level Authorization (BOLA) and Broken Function Level Authorization (BFLA) attempts - Mass assignment attacks - Anomalous or malicious payload patterns - Abnormal traffic spikes and behavioural anomalies - Server-Side Request Forgery (SSRF) and Injection attacks - Attacker identification details (IP address, token, user identity where available) - Impacted APIs and endpoints - Timestamp, frequency, and severity of attack events	
80	The solution shall provide an API Governance Dashboard to enforce policy-based controls and regulatory compliance. The dashboard must include visibility into: - Approved versus unapproved APIs - APIs operating without authentication & without rate limiting - Sensitive data exposure detection per API, including PII and financial data such as: PAN, Aadhaar, Card number and other regulator identifiers - Data classification per API (sensitive / non-sensitive), Schema Mismatch detection - Security policy compliance score for each API	
81	The solution shall provide API Contract and Schema Governance capabilities with a dedicated dashboard. The dashboard must support: - OpenAPI / Swagger schema validation and compliance monitoring - Detection of endpoints violating defined API schemas - Identification of unexpected or extra fields (additional Properties) - Detection of missing mandatory fields - Identification of oversized request or response payloads - Detection of responses exposing sensitive or restricted fields	
82	The solution shall provide an API Risk Scoring Dashboard that dynamically calculates and displays risk scores for each API. The risk scoring model must consider, at a minimum: - Authentication and authorization status - Sensitive data exposure - Traffic anomalies and abuse patterns, Detected vulnerabilities, Schema and contract violations - Public versus private API exposure	
83	Ability to validate & protect API Traffic with Encrypted Payloads	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

84	Analyse behavioural / functional patterns in API request - highlight potential fraudulent API requests in payment APIs - Analysis of consumption patterns	
85	Analyse Authenticated BOT traffic hitting APIs -multiple APIs / single API -highlight top types of bot/api attacks on infrastructure/api end points -highlight which APIs are affected by a specific type of bot attacks -extract IP address of BOT, and distinguish whether the source of bot traffic is a registered partner/client	
86	Solution should be able to show case API inventory which includes shadow API/zombie api's 1. Detect new APIs even if not on API Gateway / middleware 2. Provide visibility into security of API inventory 3. Should Support IPv4 and IPv6	
87	Solution should be flexible for - Flexible Alert and Report configuration capability - Generation of meaningful and actionable alerts / reports	
88	Solution should have the capability of creating API related Threat Model in use with historical data and run time analysis	
89	Generate alert for sensitive data movement and should have facility to whitelist the same if required	
90	Solution should be capable of Analysis of misconfiguration during implementation of API security: 1. Detect if any APIs are misconfigured and are prone to abuse 2. Recommendations should be provided to fix the API security misconfiguration / actions to improve security posture. 3. Configurable API security dashboard	
91	Solution has the provision to categorize the APIs in risk categorization like High, Medium and Low	
92	Solution should be able to capture APIs through North-South and East-West Traffic and able to generate the schema of the APIs	
93	The solution shall provide API security, including support for importing API definitions via Swagger/OpenAPI specifications	
94	For DNS, CDN, WAAP, and Advanced Bot Solutions, all logs should be stored on cloud storage for 180 days and Log data storage and processing should only occur within India.	
95	Teams should be provided Named Human Resources & comprehensive OEM Team throughout the project (Account Manager, Engagement Manager, Pre-Sales, Client Service Manager, Technical Project Managers, Solutions Architect, Security Consultants/Architects).	
96	The OEM shall provide the highest available support tier (e.g., *Premium / Elite / Platinum*) for all production environments, including 24x7 support, defined SLA commitments, priority incident handling, and access to senior technical experts for critical security incidents.	
97	The solution must include a fully managed service for continuous identification, analysis, and remediation of false positives across all security services provided by the product (e.g., WAF, Bot Management, API Security, DDoS, CDN etc).	
98	The managed service shall cover: ○ Security policy fine-tuning and optimization ○ Bot mitigation rule calibration ○ Behavioral traffic analysis using AI/ML-based detection models ○ Log analysis and correlation	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

	○ Creation and maintenance of exceptions/whitelists wherever required This activity shall be performed on an ongoing basis to align security controls with application behavior and evolving threat patterns.	
99	SIEM Noise Reduction & Alert Quality Assurance: The OEM shall ensure that only validated, high-confidence security alerts and incidents are forwarded to the Bank's SIEM platform for further investigation, thereby reducing alert fatigue and operational overhead for the Bank's SOC team.	
100	Audit, Regulatory & Forensic Support: The OEM shall be responsible for providing supporting evidence, logs, reports, and forensic data as and when required by the Bank for internal audits, external auditors, or regulatory compliance purposes, within agreed timelines.	
101	The bidder shall provide a pre-upgrade configuration impact analysis service for all software upgrades of the proposed solution. The analysis is expected to be configuration-aware and not limited to generic release notes or publicly available documentation. Prior to any planned upgrade, the OEM shall: - Review the customer's existing configuration, enabled features, and deployment architecture. - Analyze known issues, limitations, and caveats in the targeted software version and confirm whether any such known issues are applicable to customer's configuration. - Provide documented recommendations, including risk areas, prerequisites, and mitigation steps.	

Annexure 2 : Regulator requirement in DNS Management (Mandatory)

Sl	**Requirements**	Compliance-Yes/NO
1	The existing and future Name Server IP addresses (both IPv4 and IPv6) must be resolved within India, in compliance with regulatory guidelines.	
2	The existing and future Name Server hostnames must be customizable as per the Bank's requirements	
3	The IP addresses (IPv4 and IPv6) assigned to each Name Server must be unique and dedicated to South Indian Bank	

Annexure 3: The tentative scope of work

No	**Requirement**	
	Scope of Work	
	General Requirements	**Compliance -Yes/No**
1	All the existing applications (mobile and web) currently hosted in Bank's on premise WAF device should be migrated to the proposed SaaS based DDoS, WAF, Anti-Bot, CDN service & API Security Solution.	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

2	DDoS, WAF, Anti-Bot, CDN service & API Security Solution design service. The Business model for the services should be the fully loaded product from OEM.	
3	Capable for implementing API security solution in aligned with Proposed SaaS model as per bank requirement.	
4	DDoS, WAF, Anti-Bot, CDN service & API Security Solution with 5-year 24 x 7 subscription/support services.	
5	DDoS, WAF, Anti-Bot, CDN service & API Security Solution cloud License with 5-year 24 x 7 topmost support services.	
6	Installation and configuration of the provided software and hardware to implement the design.	
7	Performance tuning of all supplied cloud-based service and software for the DDoS, WAF, Anti-Bot, CDN service & API Security Solution.	
8	Training and documentation. Ongoing support.	
9	OEM-Vendor has to supply, install and maintain all the necessary Cloud Service/hardware, software and other related tools/software at SIB, which comprise the complete solution as per the requirements specified.	
10	Experienced and responsible technicians/Engineers who will be executing the project should inspect the SIB campus to evolve a clear understanding of the nature and scope of work involved.	
11	Vendor shall deploy qualified personnel at SIB to install all supplied Hardware/Software and to provide required services.	
12	Vendor shall record all major / minor incidents, which will help to take decisions on design planning, network planning and performance enhancement.	
13	Vendor should conduct periodic security and network reviews during the 5-year Subscription/warranty period and ensure all patches/upgrades are applied as and when OEM releases them.	
14	A detailed Bill of materials should be provided by Vendor.	
15	Web Application Firewall Upgrade Solution & CDN Service Design: -The Vendor is required to provide logical and physical design for the DDoS, WAF, Anti-Bot, CDN service & API Security Solution based on the following technical requirements. Hardware sizing (if any) exercise requirement must be carried out by the vendor based on the data provided in the Annexures	
16	Hardware/Appliances (if any): -The Vendor is required to propose and provide the necessary hardware appliances (if any) and associated peripherals for the setup of the DDoS, WAF, Anti-Bot, CDN service & API Security Solution. Network will be provided by SIB. However, the Vendor is required to provide the network design and specification of the equipment needed	
17	Software: - The Vendor is required to propose and provide the entire necessary cloud/software licenses for setting up the DDoS, WAF, Anti-Bot, CDN service & API Security Solution.	
18	Proof of Concept (POC): -The Original Equipment Manufacturer/System Integrator should be ready to do POC at no cost and no obligations to SIB. All necessary cloud service/equipment & software should be supplied by vendor for POC of DDoS, WAF, Anti-Bot, CDN service & API Security Solution. If vendor/OEM is not ready to carry out POC as per the terms, Bank reserves the right to reject the proposal	
19	The Vendor will be responsible for the installation and configuration of all hardware and software required and supplied	

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in

20	In the proposed DDoS, WAF, Anti-Bot, CDN service & API Security Solution, SI/OEM can provide solutions to catch API east-West traffic. To achieve API east-West traffic, SI/OEM able to provide software/Hardware within in the scope of this RFP.	
21	Configuration of the Centralized Management Console that allows the administrators to manage all modules DDoS, WAF, Anti-Bot, CDN service & API Security Solution (Hardware/Software) from one single console.	
22	Vendor should provide IBM Q radar app (if app is available) for the integration of DDoS, WAF, Anti-Bot, CDN service & API Security Solution with SIEM tool.	
23	The solution shall support log export in CEF (Common Event Format).	
24	Cloud license/Software license and hardware (if any) should be optimized.	
25	OEM should certify the design action and implementation plan.	
26	OEM should directly carryout installation and fine tuning of entire solution.	
27	OEM should visit the site after three months of go live for any final configuration and fine tuning.	
28	Configure the solution to align with security policies, compliance requirements, and operational workflows	
29	Implement real-time threat detection capabilities to identify and alert on security incidents as they occur.	
30	OEM should provide the plan for smooth transition of existing WAF & CDN service to newly proposed solution.	

22. Key Guidelines

1) The OEM shall fully comply with all requirements specified in the RFPQ. Proposal response may be submitted either directly by the OEM or through an authorized/preferred OEM partner.
2) The OEM shall remain directly responsible for end-to-end project delivery. This includes the availability of on-site resources, as required, until project completion, and the provision of all necessary technical support directly from the OEM.
3) Bidder's proposal should strictly conform to the specifications of this RFPQ. Proposals not conforming to the specifications will be rejected subject to the bank's discretion. Any incomplete or ambiguous terms/ conditions/ quotes may result in disqualification of the offer at bank's discretion. The bidder has to offer specific remarks for technical requirements and clearly confirm compliance. Any deviations on technical requirements should be clearly informed in remarks column.
4) Deviation/ comments on other terms prescribed by the bank are to be provided in a separate section in Technical Bid. The bank is not bound to evaluate the deviations mentioned at any other section of the bid.
5) Technical and Commercial bid documents are to be properly hard bound and signed by the authorized signatory under the company seal.

END OF DOCUMENT#

The South Indian Bank Ltd., Regd. Office: Thrissur, Kerala
Head Office: S.I.B. House, T.B. Road, P.B. No: 28, Thrissur - 680001, Kerala
(Tel) 0487-2420 020, (Fax) 91 487-244 2021, e-mail: sibcorporate@sib.bank.in
CIN: L65191KL 1929PLC001017, Toll Free (India) 1800-102-9408, 1800-425-1809 (BSNL)
www.southindianbank.bank.in