भारतीय स्टेट बैंक
State Bank of India
With you - all the way

REQUEST FOR PROPOSAL

Purpose: RFP for Information Security Review/Audit of Locally Hosted Critical Application for SBI Bangladesh Operations 2022-2023.

Ref: CO/SBI/IS/CSR/2022/03

Dated: 12/04/2022

1. About SBI Bangladesh

SBI's presence in the soil of Bangladesh dates back to 1862 when Bank of Bengal took over Dhaka Bank. Since then, with a brief interruption from 1962 to 1974, SBI through its Bangladesh Operations has been serving the people of Bangladesh. We recommenced our operations in 1975 by reopening our Dhaka Branch at Motijheel on 5th May 1975 after the independence of Bangladesh. Presently we are serving the nation through a network of 3 branches, 1 Banking Booth and 2 offshore Banking Units in Dhaka, Chittagong and Khulna.

Requirements

We are searching the Information Security Auditors for the year 2022-2023 The details scope of audit are given below:

2. Scope of Work:

The Auditors shall review the following Applications and the scope of work has been mentioned hereunder.

Sl No.	Application Name	Category	Risk Categorisation
1	BACH & BEFTN Interface (PBM & Application Server)	C	Medium
2	HRM Software	B	Low
3	Bulk Data Reporting System	B	Low

4	RTGS Interface	C	Medium
5	GoAML	B	Low
6	CIB	C	Low

SCOPE COVERED IN SECURITY REVIEW - parameters (but not limited to):

S. No.	Scope Area	SECURITY REVIEW Scope for ISSP
1	**Application Security Review**	Grey box testing (credentials required) Number of Input Screens, number of pages, Privilege levels, Number of Interfaces, Sequence diagram, data flow diagram, sequence Diagram, System architecture, number of modules within the application
2	**Secure Network Architecture Review**	Network Architecture diagram depicting placement of all network devices and assets like switch, router, load balancer, firewall, Web Server, App Server, DB Server, specific port numbers and protocol for communication between any two points and defining DMZ and Non-DMZ zone, as the case may be. Integration with third parties / other Networks
3	**Vulnerability Assessment**	Credential based latest VA - Raw report from SOC to be submitted by the AO to ISSP.
4	**Penetration Testing**	Internal and External PT (whatever is applicable)
5	**SCD / Configuration review**	Verification of servers' settings against Bank's latest SCD. Output of server and server component (like apache, Web logic, Oracle etc.)
6	**Integration with Security Solutions**	To ensure integration of the Application under review with all Security/ monitoring solutions including but not limited to the following are in place: SIEM integration of all Servers, PIMS integration of all Servers, DAM integration of all DB Servers, ITAM entry for all assets, AV deployment for all Servers and Desktops, Application to be registered in APM and criticality be defined by IT Risk Dept Access Management -

		PIMS/TACACS etc NAC, DLP etc
7	**Source Code review**	White Box testing. Assurance certificate of Cert-In empaneled vendor and Grey box testing, both for code not available with the Bank.
8	**API review**	Source code review and communication passing through API. This includes placement of API in the architecture.
9	**Database review**	Verify the user roles, access mechanism and mode of communication with other databases. To be specifically checked whether any direct communication with DB is present. Logging of Database events DAM Integration
10	**Process /Policy and Regulatory Compliance review**	To check existence of an approved document each with the AO and implementation vis-à- vis Bank's various policies. To check end to end communication containing encryption and/or hashing algorithm for data at rest and data in motion, mode and format of data travel, data status at different landing and storage points, mode of communication, data packet analysis,URL analysis, chances of interception of the information at any stage and manipulation etc.
11	**Firewall rule Base Review(wherever applicable)**	Verify the Firewall rules to identify Risky/Redundant rules (detailed process as per Annexure – K). All the ports need to be assessed across the rules to identify the unnecessary rules.
12	**Forensic Readiness Review**	Analyse the system to check its readiness for Logs retention, Management, Retrieval, Backup and Vendor assessment, Communication channel, and Encryption logic. SIEM Integration
13	**Vendor Integration/ Offsite Third- Party**	To check that the access is restricted to need to know basis, all the access levels need to be reviewed, Secure communication to be ensured, Logs for

	Integration(wherever applicable)	access management and changes implemented as per the details provided by AO. Security regarding data storage and server to server validation for each request to be specifically verified. Security posture of the Third party infra to be assessed through CERT-In empaneled auditor's report
14	**Integration with other internal/ External application/services/channels(wherever applicable)**	Full Details integrations with Internal/External applications/ Services/Channels. Analysis of the integration as per the Bank Policy/ for request Confidentiality, Integrity and Server-side validation. Controls in place to assure confidentiality, integrity and Server-side validation for the communication.
15	**Application Threat modelling review**	Threat modelling process followed by AO team including identification of vulnerabilities, and defining countermeasures to prevent, or mitigate the effects of, threats to the system. Analysis of threats identified and counter measures
16	**Code deployment Process**	Review of Approvals for each Change Request, Review of Record of Versions for each approved change in Non-Production and in Production, Review of the Production Deployment process, Review of Access Control to Production, Deployment Process, Verify the maintenance of relevant records to trace only security tested code is deployed in production. Record the evidence that every change request moved to production is reviewed. Log generation and review of the logs for Code deployed in production for each change.
17	**Miscellaneous review**	Any other relevant area as per Bank's policies and Industry best security standards and practices

SCHEDULE OF EVENTS

Bid Document Availability	Bidding document shall be available at website. https://bd.statebank
Last date for requesting clarification (optional)	**Up to 12 PM on 14/04/2022** All communications regarding points / queries requiring clarifications shall be given in writing to :
Clarifications to queries raised	**Within 5:00 PM, 14/04/2022**
Finalization of Audit Firm	**15/04/2022**

3. IS Audit Firm of further clarification:

Interested IS Audit Firm in Bangladesh may contact the following officials for any further clarification / information, on the date, place and time mentioned below.

The Head of IT
SBI, Bangladesh Operations.
Venue: State Bank of India
Navana Pristine Pavilion, 128 Gulshan Avenue, Gulshan 2, Dhaka-1212.

4. Professional Fees

Prices quoted in the Proposal should be excluding VAT and in BDT only.

5. Rejection of Quotation

The quotation is liable to be rejected if:

- The document doesn't bear signature of authorized person.
- It is received through Telegram/Fax/E-mail.

- It is received after expiry of the due date and time stipulated for Quotation submission.
- Incomplete/incorrect Quotation, including non –submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for Proposal are liable for rejection by SBI.

6. Extension of Deadline for submission of Bid

SBI may, at its discretion, extend this deadline for submission of quotation by amending the Documents which will be intimated through SBI website (https://bd.statebank), in which all rights and obligations of SBI and Bidders will thereafter be subject to the deadline as extended.

7. Amendment of Bidding Documents

At any time prior to the deadline for submission of Quotation, SBI, may, for any reason, whether at its own initiative or in response to a clarification requested by a Participants, amend the Bidding Documents.

Amendments will be provided in the form of Addenda/corrigenda to the Documents, which will be posted in SBI's website. Addenda will be binding on Bidders. It will be assumed that the amendments contained in such Addenda/corrigenda had been taken into account by the Bidder in its Bid.

8. Where and whom to submit the Bids:

Interested parties who are eligible are requested to submit their Quotation as per Event schedule:

The Head of IT,
State Bank of India
Navana Pristine Pavilion, 128 Gulshan Avenue,
Gulshan-2, Dhaka-1212.

The authorized representative(s) of the Company's in Bangladesh are requested to be present at the time of opening of the Technical and Commercial bids/ quotes. Maximum two representatives from a single bidder would be allowed to be present. After opening of the technical quote, evaluation would be made as per the specification

of the bank. Those who disqualify as per their technical quotes, their commercial quotes would not be opened nor would be returned.

9. Last date for Submission of the report

The last date for submission of the report will be **10th May 2022**.

- ✓ **PLEASE NOTE THE DELIVERY SCHEDULE SHALL BE FOLLOWED STRICTLY AS STIPULATED. ANY DELAY SHALL BE VIEWED SERIOUSLY AND PENALTIES LEVIED.**

10. Payment Terms

- ✓ Payment shall be made in Bangladeshi Taka.
- ✓ Payment will be released within 7 days on receipt of Invoice.
- ✓ Payments will not be released for any part-completion.

Note: Not withstanding anything said above, the Bank reserves the right to reject the contract or cancel the entire process without assigning reasons thereto.

11. FORMAT FOR TECHNICAL QUOTE: ANNEXURE -A

SL	Particulars	To be filled up by the Bidder	Whether documentary evidence is mandatory (Y/N)	If documentary evidence attached write "YES"
1	Name of the firms			
2	Constitution			
3	Year of Establishment			
4	Major activity			
5	Name of the major Banking Clients		**Y**	
6	VAT Registration No		**Y**	
7	TIN		**Y**	
8	Office Address		**Y**	
9	Firm Profile			
10	Give detailed about the Trade License		**Y**	

Locally hosted critical application Information Security Review / Audit for SBI Bangladesh Operations. 2022-2023	भारतीय स्टेट बैंक State Bank of India *With you - all the way*

I certify that the particulars mentioned above are true and correct to the best of my knowledge and believe. If it is found that any information is found to be false and or misleading, I shall be responsible for that and there would not be any liability on the Bank as a result of such misrepresentation on my part.

Dhaka

Date :

SIGNATURE OF THE BIDDER