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

REQUEST FOR PROPOSAL

Purpose: RFP for Information Comprehensive Security Review / Audit of Locally Hosted Critical Application for SBI Bangladesh Operations 2024-2025.
Ref: CO/SBI/IS/CSR/2024/01
Dated: 27/02/2024

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.

2. Requirements

We are searching the Information Security Auditors for the year 2024-2025 The details scope of audit are given below:

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 05/03/2024** All communications regarding points / queries requiring clarifications shall be given in writing to:
Clarifications to queries raised	**Within 5:00 PM, 06/03/2024**
Last Date of Submission	**10/03/2024**
Finalization of Audit Firm	**11/03/2024**

3. Scope of Work:

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

Sl No.	Application Name	Risk Categorization
1	BACH & BEFTN/NIKASH Interface	High
2	HRM Software	Low
3	RTGS Interface	High
4	GoAML	Low
5	E-KYC	Medium

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 vendor must install the application with proper approval to CBS connected desktop (whatever is applicable)
5	**SCD / Configuration review**	Verification of servers' settings against Bank's latest SCD. Output o f server and server component (like OS, DB, web, app 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 etc.
7	**Source Code review**	White Box testing. Assurance certificate of BD 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. (If Any)
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 BaseReview(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 Integration (wherever applicable)**	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 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/service /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

CSR – Scope collection document

Name of the Department:

S. No	Name of Application	No. of Devices for VA/SCD						Source Code		App sec		No. of Firewall Rules	No. of API
		OS(VA)	DB	App	Web	Others	Tot al (SCD)	LoC	Language	Privilege Level	Input pages/ dynamic pages		
1													
2													
3													
4													
5													
6													

As covered under the relevant section of Information Security Policy &Standards and Information Security Procedures and Guidelines

S. No.	Scope Area	Activity Detail	Responsibility
1	**Application Security Review**	Provide review environment (UAT/Separate Region for CSR)	AO
		Provide no. of Modules	AO
		Provide no. of interfaces	AO
		Provide no. of privileges (test credentials)	AO
		Provide no. of pages & Forms	AO
		Provide technical documentation of the application	AO
		Provide walkthrough of the application	AO
		Provide sample data	AO
2	**Secure Network Architecture Review**	Provide End to end network architecture of the application	AO
		Provide Data Flow Diagram	AO

3	**Vulnerability Assessment**	Provide OS & DB Count and IP Addresses	AO
		Placement of Servers inside network	AO
		Credentials of OS (To be input by AO in the tool)	AO
		Provide Internet facing/ Intranet facing IPs/URLs	AO
		Firewall rule approval for conducting VA within a defined time window	AO & ISD
		Installation of tools	AO & ISSP
		Provide OS & DB Count and IP Addresses	AO
		Placement of Servers inside network	AO
4	**PenetrationTesting**	Provide OS & DB Count and IP Addresses	AO
		Placement of Servers inside network	AO
		Credentials of OS (To be input by AOin the tool)	AO
		Provide Internet facing/ Intranet facing IPs/URLs	AO
		Firewall rule approval for conductingPT within a defined time window	AO & ISD
		Installation of tools	AO & ISSP
		Provide OS & DB Count and IP Addresses	AO
		Placement of Servers inside network	AO
5	**SCD / Configuration review**	SCD Version installed	AO
		OS & DB Name, Version & count	AO
		Name, version & Count of any other component	AO
		Customized SCD/Deviation Approval to be ready before review	AO
		Scripts Availability	ISD
		Methodology of SCD Review (to be advised by ISSP)	ISSP & AO
6	**Source Codereview**	Time, Date and place of readiness ofthe source code	AO
		NDA format to be signed by the vendor partner & ISSP	AO & ISSP
		No. of Line of codes & Language	AO
		Above 3 information about All the APIs exposed to others	AO
7	**API review**	Provide review environment(UAT/Prod)	AO
		Provide no. of interfaces	AO

		Provide no. of APIs(Internal/External)	AO
		Provide no. of privileges (testcredentials)	AO
		Provide technical documentation of the application	AO
8	**Database review**	List of Roles & mapping to users including DBA,	AO
		DB Access Mechanism [generic DB user/passwords],	AO
		How and in which format data is being stored in DB (specify masking and encryption details)	AO
		DB details	AO
9	**Process / Policyand Regulatory Compliance review**	User Access management	AO
		Change management	AO
		Log management	AO
		3rd party access management	AO
		Incident management	AO
		Password management	AO
		Asset management	AO
		Code management (escrow arrangement)	AO
		SLA with vendor partners (except commercials)	AO
		Backup management	AO
		Patch management	AO
		BC&OR (BCP)/ DR Plan	AO
		Version control	AO
		Threat modelling	AO
		Business approval	AO
		UAT Exit report	AO

10	**Firewall rule Base Review**	Server and desktop Asset List with segregation of PRODUCTION/DEV/SIT/UAT and also web/Application/Database	AO
		Firewall configuration file and rule base.	AO
11	**Forensic Readiness Review**	Documents related to Logs retention, Management, Retrieval, Backup and Vendor assessment, Communication channel, and Encryption logic.	AO
		logs related to the application such as User Access Logs, System Logs, Application Logs, Database logs.	AO
		Asset and Vendor list	AO
12	**Vendor Integration/ Offsite Third-Party Integration**	List of all Vendor/Offsite Third-Party integration with Application	AO
		Documents related to Network Architecture, Access Management, Patch Management, User Management, Communication Channel, Encryption, Security Controls.	AO
13	**Integration withother internal/ External application/service/channels**	Full Details of integrations with Internal/External applications/ Services/Channels.	AO
		Document related to Security Controls	AO
14	**Miscellaneous review**	Documents/processes/guidelines related to any other security challenges.	AO/ISD
		ISD In-principle approval	AO

Test for Common Vulnerabilities (including but not limited to theundernoted)

(Under each category, all possibilities and areas to be tested by the ISSP. AO should provide complete and correct information/platform for review)

(To be ensured by ISSP during review and to be included in the test cases)

S.No	Vulnerability	CSR Domain (like appsec,VA etc.)	Tested (Y/N)	Found/ Not Found
1	IDOR			
2	Cross side scripting			
3	Cross side referencing			
4	Reverse engineering			
5	Privilege escalation			
6	Hard coded values (URL/ID/Password etc.)			
7	Back button enabled			
8	Insecure Session management			
9	Information in Browser memory (Period & format)			
10	Temporary files present			
11	Data packet Capturing			
12	Insecure Encryption & Hashing for data in motion and data at rest			
13	Injection attacks			
14	Broken authentication			
15	CSRF			
16	Buffer overflow			
17	Whitelisting/Blacklisting			
18	Insecure error management			
19	Sensitive data exposure			
20	Function level access control			
21	Security controls for every layer under 07 OSI layers			
22	Week SSL Ciphers			
23	Certificates (SSL, TLS etc.)			
24	Direct DB Access (DML & DDL)			
25	Insufficient/NIL Logging			
26	Week Request & Response mechanism			
27	Use of components with known vulnerabilities			
28	Malicious file execution			
29	Security misconfigurations			

30	Non-validated redirections/forwards			
31	Probability of high jacking security of admin module			
32	Banner grabbing			
33	Use of freeware/unauthorized software			
34	Availability of version control			
35	Key management			
36	Directory listing			
37	Parameter manipulation			
38	MITM attack probability			
39	Insecure/unwanted ports open			
40	OS Level firewall management			
41	Implementation of patch (OS/DB/Physical equipment/AV etc.)			
42	SOC, PIMS, DAM integration for log monitoring			
43	ITAM Integration for asset monitoring			
44	Segregation of duties			
45	Secure environments (Dev/SIT/UAT/ISD/Pre-prod/Prod/DR etc.)			
46	Session Replay attack			
47	Copy & paste functionality enabled or not. If yes, where found			
48	Direct access to logs like App, DB, OS etc.			
49	DBLink used			
50	Cookies management			
51	Whether GET method disabled and POST method enabled			
52	Malicious file upload probability			
53	Server validation for (i) Origin of message (ii) Whether every request has been originated from genuine source			

For Mobile Applications, the following should be tested
App Authenticity
Installation on Jailbroken device
Code Obfuscation
ISSP has to include all above areas under common vulnerabilities and has to confirm pointwise in its report indicating whether done or not, observation found or not, if observation is found, reference indicating the specific page of report is to be given.

Review Plan (Schedule Chart) – Approx. estimation

(To be filled by ISSP in consultation with AO)

S.No	Application Name	Component (like Appsec, VA etc.)	Start Date	End Date	Conf. Start date	Conf. End date	Report date	AO Name (SBI Official)
			(AO)	(ISSP)	(AO)	(ISSP)	(ISSP)	
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								

Tools to be installed: - (to be filled by ISSP)

S.No.	Name of Tool	Pre-requisites, if any

1. UAT Exit Date:
2. Setup ready for review by (date):
3. Documents for SNA & Process review will be ready by (Date):

CLASSIFICATION OF CRITICALITY

Risk Rating = Likelihood * Impact	
Likelihood	This is a measure of how likely this particular vulnerability is to be discovered and exploited by an attacker. It is the combination of Method of Exploitation, Ease of Discovery & Ease of Exploit
Impact	Technical impact is to estimate the magnitude of the impact on thesystem if the vulnerability were to be exploited.

Method of Exploitation	Ease of Discovery	Ease of Exploit	Overall Likelihood
Remote Exploitation (Physical Access isnot required to the target/user's machine)	Easy	Easy	High
	Easy	Moderate	High
	Easy	Difficult	Medium
	Moderate	Easy	High
	Moderate	Moderate	Medium
	Moderate	Difficult	Low
	Difficult	Easy	Medium
	Difficult	Moderate	Low
	Difficult	Difficult	Low
Local Expl oitation (Physical Access is required to the target/user's machine)	Easy	Easy	Medium
	Easy	Moderate	Medium
	Easy	Difficult	Low
	Moderate	Easy	Medium
	Moderate	Moderate	Low
	Moderate	Difficult	Low
	Difficult	Easy	Low
	Difficult	Moderate	Low
	Difficult	Difficult	Low

OVERALL RISK RATING = LIKELIHOOD * IMPACT		
LIKELIHOOD	**IMPACT**	**RISK RATING**
HIGH	HIGH	HIGH
HIGH	MEDIUM	HIGH
HIGH	LOW	MEDIUM
MEDIUM	HIGH	HIGH
MEDIUM	MEDIUM	MEDIUM
MEDIUM	LOW	MEDIUM
LOW	HIGH	MEDIUM
LOW	MEDIUM	MEDIUM
LOW	LOW	LOW

SOURCE CODE REVIEW

1. Applicability

Applicable to all applications used in the Bank within India
Applicable to all the applications in use at the Bank's Foreign Offices, to be used as a baseline, with provision to add local regulatory requirements separately, if any.
Applicable to associates, joint ventures, subsidiaries in India and abroad, as the baseline.

2. Application Classification

Source Code of the applications may be classified in the under noted categories which may be subject to the review:

Sl No	Category	Availability of the Source Code
1	A	Application developed in-house by the Bank and Source code is available with the Bank
2	B	Application developed in-house in co-ordination with technology partner and Source Code is available with the Bank
3	C	Application developed by the technology partner at their end and Source Code is available with the Bank
4	D	Application developed by the technology partner and Source Code is available with them
5	E	Products / Software solution procured by the Bank on licensed basis, like Anti-Virus solution, ITAM, ITSM, DLP, NAC, PIMS etc. and where no source code is available with the Bank.
6	F	Applications purchased off-the-shelf whose customization is done in the Bank and no source code is available with the Bank.
7	G	Applications purchased off-the-shelf without any customization for the Bank and no source code is available with the Bank.
8	H	Operating System like WINDOWS, LINUX etc. Database like Oracle etc. Freeware tools

3. Procedure

The outlined procedure is applicable for all the applications falling under the category

A, B, C and D in the above table

For the applications under the category E, depending on the terms and conditions of the SLA, the source code review may be conducted by the Bank or the Vendor may submit the source code review report duly reviewed by a CERT-IN empaneled Security Service Provider.

For the application under category F and, Self-certification should be obtained from all entities whose products / software solutions are procured by the Bank on licensed basis.

For the applications under Category G, the portion of the source code available with the Bank shall be governed by this SOP. For the applications under category H, a self-signed certificate (format approved by IT Risk) should be obtained.

Following are the guidelines to be followed for the source code review activity:

1. Scope of work should contain the following details at minimum:

    a) Application version

    b) Code attributes (Number of lines, size, number of files)

    c) Language framework / platform

    d) Hash value of the source code & compiled code

    e) Third party libraries used (commercial / open source etc...)

    f) Out of scope files (images, static files etc.)

Source code vulnerabilities identification includes, but not limited to:

- **Usage of dangerous functions:** Certain functions behave in dangerous ways regardless of how they are used (e.g. “gets ()” in C++).

- **Bad coding practices:** Certain programming practices are prone to error and may create vulnerabilities in the software (e.g. usage of socket-basedcommunication in web applications).

- **Unvalidated input data:** An input that has not been validated prior to processingmay lead to serious security implications, such as SQL and command injections.

- **Leftover debug codes:** Debug codes may provide unintended entry points intothe applications. These may potentially be used by malicious attackers to gain access to the applications.

- **System information leakage:** Revealing unnecessary system information mayaid malicious attackers to understand the application and plan their attack.

- **Poor error handling:** Overlooking error handling may result in software going into unexpected states or conditions. This may potentially create additional vulnerabilities in the software.

• **Command/SQL injection:** Construction of dynamic SQL statements and commands using user input may lead to serious vulnerabilities.

• **Cross site scripting:** Sending invalidated data to the browser may result in execution of malicious codes at the user end.

2. Weak password management and encryption Password management issues,like storing credentials in plaintext in a configuration file, may lead to system compromise.
3. Source code design analysis should be performed to determine the design flaws
4. Source code scan should be configured based on the following parameters
    a. Compliance mandates
    b. Policies
    c. Industry best practices (to find following vulnerabilities at the minimum) :-
        i. Hardcoded account number/ other PII/SPDI
        ii. Hardcoded URL
        iii. Hardcoded user-id
        iv. Hardcoded password
        v. Scripting error resulting into a security breach
        vi. OWASP vulnerabilities
5. Perform automated scanning and verification using Source Code analyzer solution
6. Monitor scan progress and perform verification of scan completion for accuracyand completeness
7. Assign Severity and Priority to each vulnerability identified according to the application criticality to the business, network zone placement, Impact, access vector and complexity of the exploit
8. Perform thorough analysis of the Source code analyzer output and eliminate the False Positives and arrive at True Positives which requires remedial actions
9. Map the identified vulnerabilities against leading practice such as OWASP, SANS etc.
10. Collect the evidences and document detailed proof of concept where required
11. Prepare detailed technical report covering findings, observations, gaps, risk rating and recommendations
12. Prepare “Executive Summary” report for the management
13. Perform the confirmatory source code review activity as requested by the Application Owner.

FORMAT OF REPORTS

VULNERABILITY ASSESSMENT

Host
Protocol
Port Number
Plugin Output
Synopsis
Vulnerability
Vulnerability Description
Severity of Risk
Recommendation
See Also
Remarks

PENETRATION TESTINIG

Affected Servers / IP
Port
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
Remarks
See Also

APPLICATION SECURITY REVIEW

Type of Application
Platform Android/iOS/Web
Application URL
Affected Servers
Port
Whether APIs are used
If Y, No of APIs
Specify the protocol of connection (SOAP, REST, JSON, etc)
Owner of the API
Is the API consumed externally / internally
Number of APIs reviewed
Type of API and Numbers
Vulnerability

Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

SOURCE CODE REVIEW

Hash Value at Initial Review
Hash Value at confirmatory Review
Number of Lines of Code at Initial Review
Number of Lines of Code at confirmatory Review
Vulnerability
Vulnerability Description in Detail
Source File Path
Source Filenames
Source Line
Destination File Path
Destination Filenames
Destination Line
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

SECURE CONFIGURATION DOCUMENT REVIEW

Control Point
Description of Control Point
Type of System (OS / DB / N/w, etc.)
Name and Version Number
Type of Environment
IP Address
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

NETWORK ARCHITECTURE REVIEW

Point/Area of Observation
Type of System (Router / Switch / Load Balancer / port, etc....)
Name / Make / value of the system
Network Perimeter
List all stakeholders in the architecture
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

PROCESS REVIEW

Name of the Document (Access / Database Mgmt, DC / DR plan, etc....)
Version Number
Date of Document
Whether Approved
Approving Authority
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

DIGITAL FORENSIC READINESS ASSESSMENT (DFRA)

Type of System (OS / DB / N/w, etc…)
Name and Version Number
Type of Environment
IP Address
Name of Log
Whether enabled?

Log Backup
Date of last log backup
Central storage of log
Whether Log Backups are stored with Hash Value
Whether Log Backups are stored in encrypted format
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

DATABASE (DB) REVIEW

DB Type
DB Version Number
Type of Environment
Managed By
Admin privilege of the OS of DB server with
Whether OS Admin integrated with PIMS?
If Y, Is PIMS integration with password vaulting?
Admin privilege of the DB with
Whether DB Admin integrated with PIMS?
If Y, Is PIMS integration with password vaulting?
Rights of DB admin
Whether the DB access is only via application for the non-admin users
If N, specify the type of users
Whether data at rest is encrypted
Specify the algorithm
Specify encryption key location
Specify encryption key user access details
Is Data backup taken?
Specify Frequency and Location
Are backups tested
Specify Frequency
Is Data archived?

Specify Frequency and Location
Any other observation, pl specify
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

DATA FLOW DIAGRAM (DFD) REVIEW

Is the data in motion encrypted
Specify Encryption algorithm
Is the data in motion hashed?
Specify Hashing algorithm
Whether data / information is passed to third party vendor?
Does the third party have its own IS policy
Does the third party have a separate IS team
Is the data stored at third party location?
Location of data at third party
Location of Cloud
What is the periodicity of the storage?
Is the third party allowed to store the data?
Specify the sensitive information stored / transmitted / processed at thirdparty
Specify the controls at third party to protect CIA of Banks data
Specify how is the bank information segregated from the other customersinformation?
Is the Bank data shared to any other external parties by the third party?
If Y, Does the third party have permission to share Bank data?
Is the security review of third-party environment conducted?
Are the reports of the review available?
Does the third party have an incident handling and reporting system?
Does the third party take prior approval from Bank for processing Bankdata in their environment
Is sub-contracting for the processing / sharing / storing Banks dataallowed by Bank

Is the architecture three tier at vendors end
Does the Bank have the right to audit a third party?
Whether vendor environment protected at perimeter level?
If yes, specify the controls
Vulnerability
Vulnerability Description in Detail
Severity of Risk
Likely Impact
Recommendation
See Also
Remarks

4. **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 Joint AVP of IT

SBI, Bangladesh Operations.

Venue: State Bank of India

Navana Pristine Pavilion, 128 Gulshan Avenue, Gulshan 2, Dhaka-1212**.**

5. Professional Fees

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

6. <u>Rejection of Quotation</u>

The quotation is liable to be rejected if:

- The document doesn't bear the signature of the 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.

7. <u>Extension of Deadline for submission of Bid</u>

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.

8. 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 on SBI's website. The 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.

9. Where and whom to submit the Bids:

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

VP OPs,

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. A maximum of 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 they be returned.

10. Last date for Submission of the report

The last date for submission of the report will be **10th Mar 2024**.

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

11. 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: Notwithstanding anything said above, the Bank reserves the right to reject the contract or cancel the entire process without assigning reasons thereto.

12. 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**	

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