REQUEST FOR PROPOSAL

VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) FOR THE SERVICES AND SOLUTIONS
OF SOCIAL ISLAMI BANK LIMITED, HEAD OFFICE, DHAKA.

Issued on: 22/09/2019

Table of Contents

INTRODUCTION AND BACKGROUND

PURPOSE OF THE REQUEST FOR PROPOSAL

This Request for Proposal (RFP) is being issued for the, Penetration Testing of Information Technology Infrastructure, as part of regular process of verifying the implemented security controls and thus to further enhance the security of the IT systems and achieve improved and secure IT infrastructure. SIBL invites technical and financial proposal from vendors for the execution of the Penetration Testing of IT infrastructure. The proposal should include the timelines and execution schedule.

The goal of this exercise is to ensure that reasonable protection is in place for general and particular threats that may exist for SIBL's IT systems and infrastructure including but not limited to the following:

1. To test and verify the security of the Information Technology systems and network so as to ensure the effectiveness of deployed security measures.
2. Verify the perimeter security controls.
3. Verify the security setup and configuration of internal SIBL's IT infrastructure. It will include the associated networks and systems with a perspective of ensuring Confidentiality, Integrity and Availability (CIA) and authenticity of data and information systems.
4. Verify the security associated with web applications / website of SIBL.
5. Identify and recommend safeguards, suited to SIBL's environment, with the aim to strengthen the level of protection of the SIBL's IT infrastructure.

These activities are part of SIBL's ongoing risk management program and are focused on identifying the risk level SIBL is currently exposed to so that an appropriate set of responses to those threats can be developed.

SIBL is seeking to identify and select an outside independent organization to perform the activities listed above. SIBL also wish to strengthen and equip IT Team gradually to improve Information Security. The remainder of this document provides additional information that will allow a service provider to understand the scope of the effort and develop a proposal in the format desired by SIBL.

TECHNICAL CONTACT

Any questions concerning technical specifications or Statement of Work (SOW) requirements must be directed to:

Name	MD. SULTAN BADSHA
DESIGNATION	EXECUTIVE VICE PRESIDENT & CITO
Address	19th fl, City center, 90/1, Motijheel C/A, Dhaka-1000
Phone	16491 or 09612001122 Ext 50150 or 50154
Email	sultan.badsha@sibl-bd.com or tanvir.khan@sibl-bd.com

DUE DATES

A written confirmation of the Vendor's intent to respond to this RFP is required by Social Islami Bank Ltd. All proposals are due by 30th September 2019 till 3 pm. Any proposal received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late proposals will not be evaluated for award.

SCHEDULE OF EVENTS

Event	Date
1. RFP Distribution to Vendors	22nd September 2019
2. Written Confirmation of Vendors with Bid Intention	06th October till 6.00 PM
3. Questions from Vendors about scope or approach due	7th October till 3.00 PM
9. Anticipated commencement date of work*	To be mentioned by bidder.

* Commencement date may vary.

GUIDELINES FOR PROPOSAL PREPARATION

PROPOSAL SUBMISSION

Award of the contract resulting from this RFP will be based upon the most responsive Vendor whose offer will be the most advantageous to SIBL in terms of cost, functionality, and other factors as specified in this RFP.

SIBL reserves the right to:

- Reject any or all offers and discontinue this RFP process without obligation or liability to any potential vendor,
- Accept other than the lowest priced offer,
- Award a contract on the basis of initial offers received, without discussions or requests for best and final offers, and
- Award more than one contract.

Vendor's proposal shall be submitted in several parts as set forth below. The vendor will confine its submission to those matters sufficient to define its proposal and to provide an adequate basis for SIBL's evaluation of the Vendor's proposal.

In order to address the needs of this procurement, SIBL encourages Vendors to work cooperatively in presenting integrated solutions. Vendor team arrangements may be desirable to enable the companies involved to complement each other's unique capabilities, while offering the best combination of performance, cost, and delivery for the Penetration Test being provided under this RFP. SIBL will recognize the integrity and validity of Vendor team arrangements provided that:

- Vendor's adequate skill will be assessed and tested by SIBL. Certification or accreditation may not be the only qualification to win the VAPT project

Vendor's proposal in response to this RFP will be incorporated into the final agreement between SIBL and the selected Vendor(s). The submitted proposals are suggested to include each of the following sections:

1. Executive Summary
2. Approach and Methodology
3. Project Deliverables
4. Project Management Approach
5. Detailed and Itemized Pricing
6. Appendix: References
7. Appendix: Project Team Staffing
8. Appendix: Company Overview

The detailed requirements for each of the above-mentioned sections are outlined below.

DETAILED RESPONSE REQUIREMENTS

EXECUTIVE SUMMARY

This section will present a high-level synopsis of the Vendor's responses to the RFP. The Executive Summary should be a brief overview of the engagement, and should identify the main features and benefits of the proposed work.

SCOPE, APPROACH, AND METHODOLOGY

Include detailed testing procedures and technical expertise by phase. This section should include a description of each major type of work being requested of the vendor. All information that is provided will be held in strict confidence. The proposal should reflect each of the sections listed below:

- Dynamic vulnerability scanning.
- Security Architecture review
- Threat Modeling
- External Network Vulnerability Assessment and Penetration Testing
- Internal Network Vulnerability Assessment and Penetration Testing
- Web Application Manual Penetration Testing
- DMZ or Network Architecture Designs / Reviews
- Virtual Infrastructure Security Assessment
- Server Configuration Reviews
- Database security Assessment
- Firewall and Router Configuration Reviews
- VPN Configuration Reviews

DELIVERABLES

Include descriptions of the types of reports used to summarize and provide detailed information on security risk, vulnerabilities, and the necessary countermeasures and recommended corrective actions. Include sample reports as attachments to the proposal to provide an example of the types of reports that will be provided for this engagement.
Vendors will provide reports in three separate files:

1. Executive Summary report
2. External VAPT report
3. Internal VAPT report

In "Executive Summary" deliverables will be

a) Purpose, Methodology and Scope of work for External and Internal Penetration Testing
b) Penetration Testing tools used
c) Overall Evaluation Summary of observation risk severity (High, medium, low etc.) along with pie chart presentation

In "External Penetration Testing" and "Internal Penetration Testing" reports, the technical details of the test will be documented. The following elements must be brought in these reports:

a) Objective, scope, summary of findings, Risk rating and Likelihood Criteria
b) Detailed technical report for each host under the scope
c) In technical details report there must Host identification, number of vulnerabilities and type of vulnerabilities, open ports, active services by enumeration action.
d) Graphs representing risk severity level must be present
e) Vulnerability Details of hosts along with assigned risk grade and Likelihood grade will be presented
f) Remediation of each vulnerability will be presented
g) Annexure that showing up step by step penetration attempts to each vulnerability found and identify as threat.

Achievement of the following scenario would qualify as successful penetration:

- Access to internal resources (like file server, DNS or mail server, Web application server etc).
- Reading restricted files (reading / browsing restricted folders, Web application files, OS critical files etc).
- Reading transaction data.
- Access to any user account.
- Escalating privilege of lower privileged user account, in case of white box testing
- Gain Access to administrative accounts.
- Gaining access to network management systems.
- Demonstrating ability to control resources (like desktops, servers, devices etc).
- Exploiting any of the OWASP top 10 vulnerability.

In case of successful penetration, pen tester MUST not alter any data or do any activity which may cause unwanted disruption. Pen tester MUST keep evidence and Present it to IT Team as well as include evidence in Report.

PROJECT MANAGEMENT APPROACH

Include the method and approach used to manage the overall project and client correspondence. Briefly describe how the engagement proceeds from beginning to end.

DETAILED AND ITEMISED PRICING

Include a fee breakdown by project phase and estimates of travel expenses.

CURRENCY

All price must in Bangladeshi Taka.

VAT & TAX

All price must include VAT & Tax as per government policy.

ADDRESSES TO :

The Executive Vice President & Head
ICT Division, City Center, Level 19, 90/1, Motijheel C/A
Dhaka-1000

SENT TO:

The Senior Executive Vice President & Head
Logistics Support Division, City Center, Level 29, 90/1, Motijheel C/A
Dhaka-1000

APPENDIX: REFERENCES

Provide three (3) Bangladeshi Bank's references for which you have performed similar work.

APPENDIX: PROJECT TEAM STAFFING

Include biographies and relevant experience of key staff and management personnel. Describe the qualifications and relevant experience of the types of staff that would be assigned to this project by providing biographies for those staff members. Describe bonding process and coverage levels of employees. Affirm that no employees working on the engagement have ever been convicted of a felony.

Section A: General Information

1	Name of the Bank		Social Islami Bank Limited				
2	Procuring Entity Name		Logistic Support Division				
3	Invitation of tender for		VULNAREBILITY ASSESSMENT AND PENETRATION TESTING (VAPT) SERVICE AND SOLUTIONS FOR SOCIAL ISLAMI BANK LIMITED, HEAD OFFICE, DHAKA as per technical specifications detailed in "Section C" hereunder from the eligible and enrolled/ registered vendors/ suppliers/ distributors/ local agents as per "Section C" hereunder.				
4	Invitation for Quotation Ref. & Date		SIBL/HO/LSD/2019/1674 date: 22.09.2019				
5	Procurement Method		Open Tendering Method				
6	Source of Fund		Social Islami Bank Limited				
7	Tender Security (conditionally **refundable**)		Tk. 1.00 lac (Taka One lac) The tender security shall be deposited in the form of Payment Order (conditionally **refundable** either partly or in full) favoring "Social Islami Bank Limited".				
8	Registration of bidders & price of Tender Document:		The interested eligible bidders have to enroll their name by submitting a prayer along with a non-refundable registration/enrollment fee Tk 2,000.00 (Taka Two thousand) only in the form of "Payment Order" in favor of "Social Islami Bank Limited before submission of tender. No Tender documents will be sold physically. The bidder have to copy or download this tender documents from the website: www.siblbd.com and place them on their own letterhead to submit their bid.				
9	Important Tender Process Dates & Times	Tender Process	Registration		Submission		Opening Time
			Start	End	Start	End	
		Date	22.09.2019	06.10.2019	07.10.2019	07.10.2019	07.10.2019
		Time	10.00 am	6:00 pm	10:00 am	3:00 pm	3:30 pm
10	Tender Validity		3 (Three) months from the date of submission.				
12	Place of opening tender documents		Social Islami Bank Limited, Level-29, City Centre, 90/1, Motijheel C/A, Dhaka-1000				
13	Composition of bid Price shall be inclusive of		The costs of complete VA and PT and admissible VAT, excise duty, subsidiary duty, import duty, ATV, AIT etc all types of taxes and revenues of the government and other regulatory authorities along with time value of money up to settlement of bills taking clearances from the end user of the bank.				
14	Delivery Address		Social Islami Bank Limited, Level-19, City Center, Dhaka-1000.				
15	Mode of payment		i. 50% of the payment will be made after performing VA & submission of report ii. 50% of the payment will be made after PT and submission of report.				
16	Submission of bidders qualifications/ eligibility and oath of bidder		The interested registered bidder shall copy the "bidders' qualification" form from the webpage and place them on their own letterhead write their qualifications and individual information in the designated fields and submit the form along with the supporting documents as proof of the provided information.				
17	Submission of Technical Specifications		The interested registered bidder shall copy the Asked Technical Specifications form from the webpage and place them on their own letterhead write their own specifications and part numbers in the designated fields and				

		submit the document along with the supporting original brochure, detail color picture in a separate sealed envelope with proper labeling mentioning- "VULNAREBILITY ASSESSMENT AND PENETRATION TESTING (VAPT) SERVICE AND SOLUTIONS FOR SOCIAL ISLAMI BANK LIMITED, HEAD OFFICE, DHAKA", Name of the bidder & Registration No. All the bidders have to submit the softcopy of their personal data and technical offers in a readable CD/DVD ROM along with the technical offer and send a copy of the same after opening of the tender to the email address: lsd@sibl-bd.com .
18	Submission of Financial Offer	The interested registered bidder shall copy the Financial Offer form from the webpage and place them on their own letterhead and write their price offer for Section D in the designated field(s) and submit the document in a separate sealed envelope with proper labeling mentioning- "Financial Offer- for VA and PT for SIBL".
19	Name and address of the Office for receiving tender(s)	Senior Executive Vice President and Head Logistic Support Division Social Islami Bank Limited Level-29, City Centre, 90/1, Motijheel C/A, Dhaka-1000
20	Address of Official Inviting Tender	Do.
21	Contact Details	Telephone No. 09612001122- Ext: 50154,50299, email: lsd@sibl-bd.com
22	Special Instruction	This Request for Proposal shall become part of the contract and will be in effect for the duration of the Contract period.
		The successful bidder will be required to enter into and sign a formal Contract with the Bank with reasonable adjustments acceptable to the Bank. The agreement will become a part of the Contract and will be in effect for the duration of the contract period. The contract language will control over any language contained within this RFP that conflicts with the signed and fully executed Contract. Standard format of an NDA must be submitted with the proposal.
		The Bank Authority reserves the right to - 1. Explain or clarify the terms of this tender notice in its own way, 2. Bring necessary changes in the notice 3. Increase or decrease the tender quantity 4. Reject the lowest, 5. Reject any or all bids, 6. Select any bidder deems fit and proper by them The bank authority can perform all the above things without assigning any reason. The bidder/supplier shall have no right to challenge the decision of the Bank Authority in any court of law or to any arbitrator.

EVALUATION FACTORS FOR AWARD

The technical proposal and the financial proposal of a bidder will be evaluated separately. The evaluation criteria and the relative weight for each criterion are given below. SIBL reserves the right to change the evaluation criteria and the weights if it feels to do so for the benefit of the Bank.

Section B: Bidder's Information and Qualifications/Eligibility

SN	Description	Qualification	Response	Remarks
01	Name of the Bidder	Required		Attach NID copy
02	Designation of the Bidder	Required		
03	Company Name	Required		
04	Company Type	Required	Proprietorship, Partnership, Private Limited, Public Limited etc	
05	Website address of the company	Required		
06	Bidder's Office Phone No.	Required		Attach bill copy
07	Bidder's email address	Required		Send "Hello" mail to lsd@sibl-bd.com
08	Bidder's Mobile No.	Required		
09	Verified Business Address	Required		Attach proof
10	Name of Contact Person	Required		Attach NID copy
11	Designation of the contact Person	Required		
12	Official email address	Required		Send "Hello" mail to lsd@sibl-bd.com
13	Valid Trade License No.	Required		Attach proof
15	Valid VAT Registration No.	Required		Attach proof
15	Valid ETIN	Required		Attach proof
16	The bidder should be a company registered and working in Bangladesh for at least 2 years.			
17	Bank solvency certificate	Required		Attach proof
18	Experience: Bidders should have performed Penetration Testing & Vulnerability Assessment, Security audit and Application Control review for at least 3 (three) Banks in Bangladesh. Experience/reference must be submitted.	Required Bank- WO- Date- Quantity		Attach proof
19	The Bidder may have Team Leader for this project with IT-related or engineering education and a CISSP/CISM certification with 5 years of Information Security and IS Audit experience. Working experience of Information Security in the Bank or Telecom Operator is preferred.			Attach proof

20	Team MUST have 1 LPT (Master), 1 CCISO and 1 CEH			Attach proof
21	Company being ISO 27001 certified will get preference.			Attach proof
22	Are you Banned by any bank authority or government agency?	Yes/No		

Statement of the bidder: All the above information provided hereinabove are true. We will supply the order from genuine, valid and lawful sources and will pay all admissible VAT, Tax & other duties as per rule of the Government of Bangladesh.

Technical Scoring

The bidder's technical offer will be opened first. Below are the evaluation criteria of Technical bid.

Sl	Major	Evaluation items	Remarks	Total
01	Requirement	Compliance of requirement	-	10
02	Reference client	Experience on Vulnerability Assessment & Penetration Testing in Bangladeshi Banks, NBFI and Telecom Organization within last 2 years.	5 Points for each qualified Organization Maximum Number can be achieved is 20	20
03	Vendors organization capacity	02 (Two) Team members who were recognized and appreciated by Google, twitter, Facebook or other fortune 500 companies for security research and listed as security researcher in their 'Hall of Fame'	1 for Each team member. Maximum Number can be achieved is 2	2
		Bidder should have valid and legitimate insurance coverage of "TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE" covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction /corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate. Coverage territory should include Bangladesh.	Copy of Insurance Policy as evidence. Full number will be provided in case of compliance.	5
		Number of LPT (Master)/OSCP in the team	Maximum 5 points	5
		Number of CEH/ECSA	1.5 point for each CEH team member	6
04	Certification	Company having ISO 27001 certified is preferred.		2
Total				**50**

REQUEST FOR PROPOSAL (RFP) SUBMISSION CRITERIA :

Submission of proposals

a. Sealed proposals will be received for providing the services/solutions/products for Social Islami Bank Limited by the Logistic Support Division of Social Islami Bank, Dhaka until (3.00 p.m.) at which time they will be publicly opened.

b. Sealed Proposals must include:
    1. Technical Proposal: one (1) original hard copy.
    2. Financial Proposal: one (1) original hard copy.

c. NOTE: Packages not containing the required number of copies will be rejected.

d. No proposal will be considered which is not accompanied by the attached Financial Proposal and signed by the proper official of the bidder. Proposals will not be accepted by FAX or email.

e. Proposals shall be received in the office of the Logistic Support Division on or before the time and date specified. Proposals received after the time specified will not be considered and will be returned unopened.

f. Financial Proposal information is restricted and will not be opened by the Technical Committee on the day of opening the technical tender documents. The Financial offers will be opened by the Purchase Committee for those bidders only who will be judged "Technically qualified" by the Bank's technical committee.

Modifications or Withdrawals of Proposals

a. A proposal that is in the possession of the Bank may be altered by letter bearing the signature or name of the authorized person, provided it is received PRIOR to the date and time of the opening. FAX, telephone, or verbal alterations will not be accepted.
b. A proposal that is in the possession of the Bank may be withdrawn by the bidder up to the time of the opening. Failure of the successful bidder to furnish the service awarded as a result of this advertisement shall eliminate the bidder from the active bidders list for a period of time as determined by the Logistics Support Division.

Preparation of Proposals

a. No proposal will be considered which modifies, in any manner, any of the provisions, specifications, or minimum requirements of the Request for Proposal.
b. In case of error in the extension of prices in the proposal, unit prices will govern.
c. Bidders are expected to examine special provisions, specifications, schedules,

and instructions included in this Request. Failure to do so will be at the bidder's risk.

d. Failure to respond to Request for Proposals will be understood by the Bank to indicate a lack of interest and will result in the removal of the Bidder's name from the applicable mailing list

SIBL may, at their discretion and without explanation to the prospective Vendors, at any time choose to discontinue this RFP without obligation to such prospective Vendors.

Section C: SCOPE OF WORK & TECHNICAL REQUIREMENT

The following information should be used to determine the scope of this project and provide pricing for this engagement:

SI	Name of the Service / System/Equipment	Name of the Component	Qty	Vulnerability Assessment (VA)	Penetration Test (PT)	Configuration Review (CR)
1	Internet Banking/ Mobile App	Operating System	7	Y	Y	Y
		Web Server	1	Y	Y	Y
		Web Application(IB)	1	Y	Y	Y
2	Core Banking Application	Operating System	1	Y	Y	Y
		Web Server	1	Y	Y	Y
		Web application	1	Y	Y	Y
3	Core Banking Database	Operating System	1	Y	Y	Y
		Database	1	Y	Y	Y
4	SWIFT	Operating System	1	Y	Y	Y
		Workstation	5	Y	Y	Y
		Application	1	Y	Y	Y
5	Active Directory & Domain Controller	Operating System-Server	3	Y	Y	Y
6	BEFTN	Operating System	1	Y	Y	Y
		Application	1	Y	Y	Y
		API	1	Y	Y	Y
7	RTGS	Operating System	1	Y	Y	Y
		Application	1	Y	Y	Y
		API	1	Y	Y	Y
8	BACH	Operating System	1	Y	Y	Y
		Application	1	Y	Y	Y
		API	1	Y	Y	Y
9	In-House Application	Web Server	5	Y	Y	Y
10	Router	Data Center (DC)Core	1	Y	Y	Y
		Disaster Recovery Site (DRS) Core	1	Y	Y	Y
11	Firewall	Internet	1	Y	Y	Y
		Data Center (DC)Core	1	Y	Y	Y
		Disaster Recovery Site (DRS) Core	1	Y	Y	Y
		WAF (DC)	1	Y	Y	Y
		DMZ (DC)	1	Y	Y	Y

Pen tester should provide Separate VA and PT report. PT report **must** include evidence of successfully exploited vulnerability. VA report should be manually verified and False positive issues should be identified and reported accordingly.

Required Security Testing criteria

For web application, pen tester should conduct but not limited to the following security testing. For Unsuccessful penetration, vendor MUST enclose evidence in the report that each of the required test was conducted for that specific web application/System/API.

SL#	Pen tester should ensure following illustrative testing along with other industry standard requirements for Web Application Security Testing	Vendor Response
1.0	**Deployment**	
1.1	Manually test for missing security updates.	
1.2	Manually test for unsupported or end-of-life software versions	
1.3	Test for HTTP TRACK and TRACE methods	
2.0	**Information disclosure**	
2.1	Test for extraneous files in the document root	
2.2	Test for extraneous directory listings	
2.3	Test for accessible debug functionality	
2.4	Manually test for sensitive information in log and error messages	
2.5	Manually test for sensitive information in robots.txt	
2.6	Manually test for sensitive information in source code	
2.7	Manually test for disclosure of internal addresses	
3.0	**Privacy and Confidentiality**	
3.1	Manually test for sensitive information stored in urls	
3.2	Manually test for unencrypted sensitive information stored at the client-side	
3.4	Manually test for sensitive information stored in (externally) archived pages	
3.5	Manually test for content included from untrusted sources	
3.6	Test for caching of pages with sensitive information	
3.7	Manually test for insecure transmission of sensitive information	
3.8	Test for non-SSL/TLS pages on sites processing sensitive information	
3.9	Test for SSL/TLS pages served with mixed content	
3.10	Test for missing HSTS header on full SSL sites	
3.11	Test for weak, untrusted or expired SSL certificates	
3.12	Test for the usage of unproven cryptographic primitives	
3.13	Test for the incorrect usage of cryptographic primitives	
4.0	**State Management**	
4.1	Manually test for client-side state management	
4.2	Manually test for invalid state transitions	

5.0	**Authentication and Authorization**	
5.1	Manually test for missing authentication or authorization	
5.2	Manually test for client-side authentication	
5.3	Manually test for predictable and default credentials	
5.4	Manually test for predictable authentication or authorization tokens	
5.5	Manually test for authentication or authorization based on obscurity	
5.6	Manually test for identifier-based authorization	
5.7	Test for acceptance of weak passwords	
5.8	Test for plaintext retrieval of passwords	
5.9	Test for missing rate limiting on authentication functionality	
5.10	Manually test for missing re-authentication when changing credentials	
5.11	Test for missing logout functionality	
6.0	**User Input**	
6.1	Manually test for SQL injection	
6.2	Manually test for path traversal and filename injection	
6.3	Manually test for cross-site scripting	
6.4	Manually test for system command injection	
6.5	Manually test for XML injection	
6.6	Manually test for xpath injection	
6.7	Manually test for XSL(T) injection	
6.8	Manually test for SSI injection	
6.9	Test manually for HTTP header injection	
6.10	Test manually for HTTP parameter injection	
6.11	Manually test for LDAP injection	
6.12	Manually test for dynamic scripting injection	
6.13	Manually test for regular expression injection	
6.14	Manually test for data property/field injection	
6.15	Manually test for protocol-specific injection	
6.16	Manually test for expression language injection	
7.0	**Sessions**	
7.1	Manually test for cross-site request forgery (CSRF)	
7.2	Manually test for predictable CSRF tokens	
7.3	Test for missing session revocation on logout	
7.4	Manually test for missing session regeneration on login	
7.5	Manually test for missing session regeneration when changing credentials	
7.6	Manually test for missing Secure flag on session cookies	
7.7	Test for missing http only Flag on session cookies	
7.8	Test for non-restrictive domain on session cookies	
7.9	Test for non-restrictive or missing path on session cookies	
7.10	Test for predictable session identifiers	
7.11	Test for session identifier collisions	
7.12	Manually test for session fixation	
7.13	Test for insecure transmission of session identifiers	
7.14	Manually test for external session hijacking	

7.15	manually test for missing periodic expiration of sessions	
8.0	**File Uploads**	
8.1	Manually test for storage of uploaded files in the document root	
8.2	Manually test for execution or interpretation of uploaded files	
8.3	Manually test for uploading outside of designated upload directory	
8.4	Manually test for missing size restrictions on uploaded files	
8.5	Manually test for missing type validation on uploaded files	
9.0	**Content**	
9.1	Manually test for missing or non-specific content type definitions	
9.2	Manually test for missing character set definitions	
9.3	Manually test for missing anti content sniffing measures	
10.0	**XML Processing**	
10.1	Manually test for XML external entity expansion	
10.2	Manually test for external DTD parsing	
10.3	Test for extraneous or dangerous XML extensions	
10.4	Test for recursive entity expansion	
11.0	**Miscellaneous**	
11.1	Manually test for missing anti-clickjacking measures	
11.2	Manually test for open redirection	
11.3	Test for insecure cross-domain access policy	
11.4	Test for missing rate limiting on e-mail functionality (if applicable)	
11.5	Test for missing rate limiting on resource intensive functionality	
11.6	Test for inappropriate rate limiting resulting in a denial of service	
11.7	Test for application- or setup-specific problems	
11.8	Provide and produce all evidence and reproduction steps for successful exploitation of vulnerabilities.	

Pen tester **MUST** conduct the following security testing for System integration/Interfacing/API

SL#	Pen tester should ensure following illustrative testing along with other industry standard requirement for API or any system integration point	Vendor Response
1.0	**API Endpoint Manual Security Testing**	
1.1	Conduct manual API Run through and provide evidentiary documentation	
1.2	Conduct manual Information Gathering on the API and provide evidentiary documentation	
1.3	Manually Map the API and provide evidentiary documentation	
1.4	Do a detailed security threat modeling	
1.5	Conduct static analysis	
1.6	Conduct dynamic analysis	
1.7	Conduct, report and suggest remediation on Business Logic Flaw Testing	
1.8	Manually verify transport layer security (Insecure Transmission) and provide evidence of manual testing along with the report	
1.9	Conduct manual verification on Authentication Security and provide evidence of manual testing along with the report	
1.10	Manually inspect and test any JSON Web Tokens and provide evidence of manual testing along with the report	
1.11	Manually validate oauth Tokens Security and provide evidence of manual testing along with the report	
1.12	Manually validate Access Controls and provide evidence of manual testing along with the report	
1.13	Manually test Input Validation parameters and provide evidence of manual testing along with the report	
1.14	Manually test non-standard parameters and provide evidence of manual testing along with the report	
1.15	Manually test all Processing parameters and provide evidence of manual testing along with the report	
1.16	Manually verify all Output data and provide evidence of manual testing along with the report	
1.17	Manually test API Error handling and provide evidence of manual testing along with the report.	
1.18	Manually verify API access rate/traffic Management and provide evidence of manual testing along with the report	
1.19	Submit a full detailed report, detailing the steps of the manual testing engagement, along with reproduction steps for each vulnerability and a suggested remediation method	

Section D: Commercial Proposal

Bidder should use the following format to submit commercial proposal.

SI	Name of the Service / System/Equipment	Name of the Component	Qty	Vulnerability Assessment (VA) Unit Price	Penetration Test. (PT) Unit Price	Configuration Review (CR) Unit Price	Total in BDT
1	Internet Banking/ Mobile App	Operating System	7				
		Web Server	1				
		Web Application(IB)	1				
2	Core Banking Application	Operating System	1				
		Web Server	1				
		Web application	1				
3	Core Banking Database	Operating System	1				
		Database	1				
4	SWIFT	Operating System	1				
		Workstation	5				
		Application	1				
5	Active Directory & Domain Controller	Operating System-Server	3				
6	BEFTN	Operating System	1				
		Application	1				
		API	1				
7	RTGS	Operating System	1				
		Application	1				
		API	1				
8	BACH	Operating System	1				
		Application	1				
		API	1				
9	In-House Application	Web Server	5				
10	Router	Data Center (DC)Core	1				
		Disaster Recovery Site (DRS) Core	1				
11	Firewall	Internet	1				
		Data Center (DC)Core	1				
		Disaster Recovery Site (DRS) Core	1				
		WAF (DC)	1				
		DMZ (DC)	1				

12	Training for ICT personnel	Bidder will provide a detailed training for the personnel of ICT Division and establish a documented process so that SIBL personnel can perform Internal periodical VA & PT as and when required. The bidder will be responsible for preparing and developing proper documentation process in this regard.					

Total : .....

VAT : .....

TAX.....

Total including VAT, TAX, AIT as applicable by Govt. rules.....

DELIVERABLES

At the conclusion of the assessment, SIBL requires written documentation of the approach, findings, and recommendations associated with this project. A formal presentation of the findings and recommendations to senior management may also be required. The documentation should consist of the following:

DETAILED TECHNICAL REPORT

A document developed for the use of SIBL's technical staff which discusses: the methodology employed, positive security aspects identified, detailed technical vulnerability findings, an assignment of a risk rating for each vulnerability, supporting detailed exhibits for vulnerabilities when appropriate, and detailed technical remediation steps.