



Social Islami Bank Limited

Logistic Support Division

Head Office, City Centre, 90/1, Motijheel C/A, Dhaka-1000

Web: www.siblbld.com; email: chspd@sibl-bd.com

INVITATION FOR TENDER

PROCURING VAPT & WEB SCANNING TOOLS

Bidder Reg. No.

Tender Ref. SIBL/HO/LSD/2023/725

Date: 11/05/2023

Publish Date	11/05/2023
Registration Close Date	08/06/2023
Submission date	11/06/2023

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	Sealed tenders are hereby invited for Procuring Vulnerability Assessment (VA), Penetration Testing (PT) & Web Scanning Tools For SIBL. As per technical specifications detailed in "Section C" hereunder from the eligible local or joint venture enterprises.				
4	Invitation for Quotation	SIBL/HO/LSD/2023/725 date: 11/05/2023				
5	Procurement Method	Open Tendering Method				
6	Source of Fund	Social Islami Bank Limited				
7	Tender Security (conditionally refundable)	Tk. 80 thousands (Taka Eighty thousands) only. 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. 1500/- (Taka one thousand five hundred) 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: https://www.siblbld.com/media#tender and place them on their own letterhead to submit their bid.				
9	Important Tender Process Dates & Times	Tender	Registration		Submission	
		Process	Start	End	Start	End
		Date	11/05/2023	08/06/2023	11/06/2023	11/06/2023
		Time	10.00 am	5.00 pm	10.00 am	3:00 pm
10	Tender Validity	Bids shall remain valid, at a minimum, for the period of 90 Days after the deadline date for bid submission.				
11	Quantity & Delivery Schedule	The successful bidder shall ensure the delivery of all devices/Products within Ninety (90) days from the date of work order and installation, configuration, testing and training shall be completed by next twenty (20) days of successful delivery. Days will be counted from the date of placement of order by SIBL to the successful bidder.				
12	Place of opening tender	Social Islami Bank Limited, Level-29, City Centre, 90/1, Motijheel C/A, Dhaka-1000				
13	Composition of bid Price	The price shall be quoted before VAT.				
14	Delivery Address	ICT Division of the bank.				
15	Mode of payment	The bill payment process may take a cycle of 45 to 60 days. The process includes the time of collecting clearances from the end users.				
16	Performance Security	The successful bidder to whom supply order will be issued shall have to submit performance security at the rate of 10% (ten percent) of the entire order amount in the form of Bank Guarantee for a period of 12 months. Otherwise, the performance security money shall be kept from the bills payable against the supply of the order.				
17	Submission of bidders qualifications/ eligibility and oath of bidder (Section B)	The interested registered bidder shall copy the "bidders' qualification" form (Section B) 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 and the tender security as specified in serial No. 7 hereinabove in a separate sealed envelope with proper labeling mentioning- "Bidder's Eligibility/Qualifications-ATM, Name of the bidder & Registration No. All papers and information shall be signed and authenticated by the bidder.				

INVITATION FOR TENDER**PROCURING VAPT & WEB SCANNING TOOLS****Bidder Reg. No.****Tender Ref. SIBL/HO/LSD/2023/725****Date:11/05/2023****Registration close date: 08/06/2023****Tender Submission Date: 11/06/2023**

18	Submission of Technical Specifications (Section C)	The interested registered bidder shall copy the Asked Technical Specifications form (Section C) 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- "Technical Specifications- Procuring Vulnerability Assessment (VA), Penetration Testing (PT) & Web Scanning Tools For SIBL. ", Name of the bidder & Reg. No. All papers and information shall be signed and authenticated by the bidder.
19	Submission of Financial Offer (Section D)	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- Procuring Vulnerability Assessment (VA), Penetration Testing (PT) & Web Scanning Tools For SIBL.", Name of the bidder & Registration No. All papers and information shall be signed and authenticated by the bidder.
20	Name and address of the Office for receiving tender(s)	Senior Vice President and Head Logistic Support Division Social Islami Bank Limited Level-29, City Centre, 90/1, Motijheel C/A, Dhaka-1000
21	Contact Details	Telephone No. 09612001122- Ext: 50291 & 50293, email: chspd@sibl-bd.com
22	Special Instruction	The Bank Authority reserves the right to - <ol style="list-style-type: none">1. Explain or clarify the terms of this tender notice in its own way,2. Bring necessary changes in the notice3. Increase or decrease the tender quantity4. 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.

Senior Vice President and Head

Logistic Support Division

Phone- 09612001122- Ext-50291, 50293

E-mail address: chspd@sibl-bd.com

INVITATION FOR TENDER

PROCURING VAPT & WEB SCANNING TOOLS

Bidder Reg. No.
Tender Ref. SIBL/HO/LSD/2023/725
Date: 11/05/2023

Registration close date: 08/06/2023
Tender Submission Date: 11/06/2023

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 chspd@siblbld.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 chspd@siblbld.com
13	Valid Trade License No.	Required		Attach proof
15	Valid VAT Registration No.	Required		Attach proof
15	Valid ETIN	Required		Attach proof
16	Valid IRC No.	Required		Attach proof
17	Authorization of the Principal	Required		Attach proof
18	Solvency	Required		Attach proof
19	Are you adequately solvent to sale on credit for a period of 6 months or more?	Yes/No.		
20	Experience: The bidder must have experience for supplying similar order in 2 different commercial Banks of Bangladesh	Required	Bank- WO- Date- Quantity	Attach proof
21	Principal's Name, Postal Address, Web address		Required	Might be verified
22	Are you Banned by any bank authority or government agency?	Yes/No		
23	Will you import the product from original equipment manufacturer? If no, who will import your products give its details	Yes/No./details		

INVITATION FOR TENDER

PROCURING VAPT & WEB SCANNING TOOLS

Bidder Reg. No.

Tender Ref. SIBL/HO/LSD/2023/725

Date: 11/05/2023

Registration close date: 08/06/2023

Tender Submission Date: 11/06/2023

Section B: Other Conditions

Item	Description	Remarks (Yes/No/comply)
Instruction to Bidders	<p>The request for proposal is consists of 03 (Three) items and the Bidder have to participate in the tender for all items or any of the Item but not any sub items. Items are:</p> <ol style="list-style-type: none"> Vulnerability Management tools Penetration Testing tools Web Application Scanning tools. <p>SIBL reserves the right to reject any or all proposals, to waive any informality or technical defect in the proposals, or to award the contract in whole or in part, if deemed to be in the best interest of the Bank to do so.</p> <p>Successful bidder must follow Bangladesh Bank's Guideline for Scheduled Banks and Financial Institutions, during device/software configuration and implementation.</p>	
Bidder Qualifications / Eligibility	<ul style="list-style-type: none"> ➤ The bidder should be a company registered and working in Bangladesh having long business track in the same type of business for which it is submitting the RFP and shall have the nationality of the People's Republic of Bangladesh. ➤ The bidder should be a manufacturer/partner/distributor/ of participated items. A copy of the necessary certification to be enclosed. ➤ The bidder should be authorized to participate in this tender. A copy of the necessary authorization letter to be enclosed. ➤ No association or consortium is allowed. ➤ Minimum three (03) years of experience in selling proposed/similar solutions. A proof of the necessary experience to be enclosed. ➤ Bidders shall have necessary financial capabilities to perform the contract, its business activities shall not be suspended, and it shall not be the subject of legal proceedings for any of the foregoing. ➤ The bidder shall not be under a declaration of ineligibility for corrupt, fraudulent, collusive or coercive practices. ➤ The bidder should have capability to provide after sales support for given solutions. ➤ Bidder must have certified engineer for offer product. A copy of the necessary certification to be enclosed. 	
Tender Submission Method	<p>Technical and Financial proposal should be submitted by the bidder in separate envelopes signed and sealed by the authorized personnel of the bidder organization. Technical Offer will contain exhaustive and comprehensive information about proposed solution and details Bill of Material & Services without pricing, whereas the Financial Offer will contain the details item wise price breakup & Services with pricing information. Sealed proposal must include (1) original and one (1) electronic copy on a CD/DVD/Flash Drive in MS-Word format. The envelopes should be marked as "Technical Proposal" and "Financial Proposal" and the name of the Bidder should be clearly marked on the envelope</p>	
Amendment to the RFP	<p>At any time prior to the deadline for submission of RFP response, the Bank may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder, amend the RFP. Amendments will be provided in the form of an addendum to the RFP and will be sent in writing or e-mail to all prospective bidders who have received the RFP and will be binding for them. It will be assumed that amendments contained in such addendums have been taken into consideration by the bidders in their response</p>	
Delay Penalty	<p>For any delay in delivery and implementation of the system solely due to failure on the part of the BIDDER, the BIDDER will be subject to penalty charges of 0.5% per week.</p>	

Order Cancellation	<p>Social Islami Bank Ltd reserves its right to cancel the order, entirely or partially, in the event of one or more of the following situations:</p> <ul style="list-style-type: none"> ➤ Delay in delivery beyond the specified period for delivery ➤ Delay in installation beyond specified date of installation. 	
Quoted Price	<p>All quoted Total Price/Amount should include delivery, installation, testing and training cost and AIT, Tax and Other Duties applicable as per Govt. rules and Bank Policy. All prices shall be quoted in Bangladesh Taka (Tk.) and the payment will be made in BDT to the successful bidders. Financial Offer must contain detail item wise price. AMC price must be mentioned with the offer according to the Schedule of Financial Proposal including Tax and other Govt. Charges. The price quoted in the financial bids would be considered as the final price for evaluation. However, BANK reserves the right to negotiate with any vendor for downward revision in the price</p>	
Warranty/Support/AMC	<ul style="list-style-type: none"> ➤ Warranty period will start from the date of commissioning and POST of the purchased server/storage. ➤ The SLA will have to be signed between Bank and successful vendor to ensure smooth support during warranty period. The bidder has to provide draft SLA covering Bangladesh Bank ICT guide line SLA clauses to cover the Warranty period support along with the offer 	
Bidding Documents	<p>Following documents must be provided with other bidding documents:</p> <ul style="list-style-type: none"> ➤ Authorization letter for signatory authority ➤ Manufacturer Authorization ➤ List of the owners of the firm/ partnership/ directors of the company. ➤ Audited Annual Report for the last financial year. ➤ Valid Trade License. ➤ TIN certificate. ➤ VAT registration certificate to be submitted. ➤ Authorized partnership/distributorship certificate of manufacturer. ➤ List of professional for maintenance and service. ➤ List of major clients in Financial Institutions and copies of certificates issued by such financial institutions regarding supply, installation and configurations of quoted solutions to such financial institutions. ➤ Project Implementation Plan ➤ UAT plan ➤ Bill of Materials (BoM) of offered products. 	
Contact Point	<p>chspd@sibl-bd.com</p> <p>Iqbal.hossain@sibl-bd.com</p> <p>Shakhawat2978@sibl-bd.com</p>	For any clarification.
Disqualification of RFP response	<ul style="list-style-type: none"> ➤ Non-compliance of the eligibility criteria ➤ Non-acceptance of complete Terms and Conditions of RFP ➤ The RFP is received in incomplete form ➤ The RFP is received after last date or time ➤ Information submitted in the technical offer is found to be misrepresented, incorrect or false, accidentally, unwillingly or otherwise, at any time during the processing of the contract (no matter at what phase) or during the tenure or the contract including the extension period if any; 	

Payment Terms	<p>The terms of payment will be as under:</p> <ul style="list-style-type: none"> ➤ After successful installation and commissioning and submission of 10% Performance guarantee for warranty period. ➤ After activation of necessary subscription/license. <p>The bidder should submit the bill with following documents:</p> <ul style="list-style-type: none"> ➤ Two Original copies of Bill ➤ Bill shall be produced with VAT 6.3 challan adding applicable VAT. ➤ Delivery Challan duly signed by ICT Division as receipt of services or materials. ➤ Copy of Work Order ➤ Certificate of installation and acceptance, signed by ICT Division to claim the bill. ➤ Income Tax and others charges shall be realized from the bill amount as per government rules and Bank's policy. 	
----------------------	---	--

INVITATION FOR TENDER
PROCURING VAPT & WEB SCANNING TOOLS

Bidder Reg. No.
Tender Ref. SIBL/HO/LSD/2023/725
Date: 11/05/2023

Registration close date: 08/06/2023
Tender Submission Date: 11/06/2023

Section C: Technical Specification

TECHNICAL SPECIFICATION

The detailed functional specifications are given hereunder. All the requirements are mandatory. Bidder shall indicate in column 3 the availability of each requirement as a standard product (S).

All the Functionalities are Mandatory and should be available in the offered solution as standard product. In case any of these are not offered as standard product, the bid may be made non-responsive.

Technical requirements summary:

Items	Name
a	Vulnerability Management tools
b	Penetration Testing tools
c	Web Application Scanning tools

Vulnerability Management Tool

SL no.	Required Technical Specification		Bidders Response	Remarks
1	Solution prerequisites: Basic Information			
1.1	Brand	To be mentioned by the bidder		
1.2	Model	To be mentioned by the bidder		
1.3	Country of Origin	To be mentioned by the bidder		
1.4	Number of IPs	512		
1.5	Deployment Type	On Premise		
2	Market Acceptance			
2.1	Proposed solution must be recognized as Leader in the Gartner report for last 3 consecutive years. (Attach proof)			
2.2	Mention other recognitions and awards for the proposed solution.			
3	Solution Requirements: Asset Discovery and Scanning.			
3.1	Asset scanning shall support the following type of checking in one single scan: - Vulnerability - Baseline Standard - Policy Compliance			
3.2	Solution Shall support the automatic discovery of following Operating Systems: - Windows Family - Linux Distribution (RedHat, Debian, Centos, Ubuntu etc.) - AIX - MAC			
3.3	Solution Shall support the automatic discovery of virtual assets on: - VMware vCenter - VMware ESX/ESXi and - Citrix XenCenter - VMware NSX - Hyper-V - Virtual / Guest Host			
3.4	Solution Shall have the functionality to perform Security Devices Scanning (e.g. firewall, WAF, Cisco ASA, Cisco WSA, Cisco ESA, load-balancer, etc.)			
3.5	Solution Shall have the functionality to granular controls scan manage speed and resource usage: Maximum retries Timeout Interval Scan Delay Packet-Per-Second Rate Parallelism Extensibility			
3.6	Shall be able to perform TCP scanning in full connection scan and stealth scan (including but not limited to SYN, SYN+FIN, SYN+RST, SYN+ECE).			
3.7	Proposed solution shall perform Internal (inside the LAN) scanning and external (outside from Firewall) scanning.			

3.8	Solution should support centralized management of distributed scan engines?		
3.9	Scans shall support credentials login to device including but not limited to CVS, FTP, HTTP, Microsoft Windows, Samba (SMB/CIFS), POP, SNMP, SSH, Telnet		
3.10	Scans shall support Agent based (host based) and Agent less (Network) scanning		
3.11	Solution should perform discovery, vulnerability and compliance assessments in a single unified scan (finding assets, vulnerabilities, and compliance audit)		
3.12	The solution should perform Intelligent port scanning for service identification running on non-standard ports and support scanning throttling/ rate limiting speed.		
3.13	The product should have the passive scanning Capability for full visibility of vulnerability.		
4	Solution Requirements: Compliance and Configuration Auditing		
4.1	Proposed solution shall provide templates for assessing policy compliance for ISO, PCI, SOX		
4.2	Proposed solution shall provide templates for assessing policy compliance for PCI, CIS, etc.		
4.3	Proposed solution support CIS, USGCB, and DISA STIGS security standards minimum		
4.4	Vendor must be one of or used by the Approved Scanning Vendor (ASV) listed in PCI SSC.		
4.5	Policy compliance testing shall include Oracle, Lotus Domino, Windows Group Policy, CIFS/SMB accounts, AS/400 and UNIX.		
4.6	Shall support custom SCAP compliance policy upload & creation		
4.7	Shall include built-in CIS Hardening Guidelines		
4.8	Proposed solution shall support customized policy		
4.9	Shall support Windows Group Policy audit.		
4.10	Provides time-based exclusion workflow for both: -Vulnerabilities - Policy Compliance Controls		
4.11	Proposed solution shall provide templates for assessing policy compliance for ISO, PCI, SOX		
4.12	Proposed solution shall provide templates for assessing policy compliance for PCI, CIS, etc.		
4.13	Proposed solution support CIS, USGCB, and DISA STIG S security standards minimum		
4.14	Vendor must be one of or used by the Approved Scanning Vendor (ASV) listed in PCI SSC.		
4.15	Policy compliance testing shall include Oracle, Lotus Domino, Windows Group Policy, CIFS/SMB accounts, AS/400 and UNIX.		
4.16	Shall support custom SCAP compliance policy upload & creation		
4.17	Shall include built-in CIS Hardening Guidelines		
4.18	Proposed solution shall support customized policy		
4.19	Shall support Windows Group Policy audit.		

4.20	Provides time-based exclusion workflow for both: -Vulnerabilities - Policy Compliance Controls		
5	Solution Requirements: Integrations		
5.1	Proposed solution shall interoperate with patch management, enterprise ticketing management, GRC, credential management, NAC and more		
5.2	APIs enable centralized management, scanning, reporting, and workflows		
5.3	Solution shall integration with virtual and cloud environments		
5.4	Solution shall integrate with different networking, firewall security solution provider.		
5.5	Solution integration with other security solutions. Please mention the security solution name.		
5.6	Solution shall support virtual patching for web application		
5.7	System shall integrate with wide range SIEM (HP, IBM, Log rhythm, RSA, etc.)		
5.8	System shall support in-build ticketing system for further investigation		
5.9	Proposed solution support integration with enterprise ticketing systems.		
6	Solution Requirements: Alerting and Notification		
6.1	Send email alerts for detected vulnerabilities during scanning		
6.2	System shall support following alert types: SMTP SNMP (v2 and above) Syslog		
6.3	Send events to enterprise SIEM systems		
7	Solution Requirements: Reporting		
7.1	Remediation reports shall provide step-by-step guide for administrators to fix the vulnerabilities found. It shall also include estimated down time as a reference for the administrators.		
7.2	Built-in reports shall include but not limited to audit, baseline comparison, executive summary, PCI, policy compliance, remediation planning, risk score card, top remediation, and vulnerability trending report.		
7.3	Base-line comparison reports shall include risk trend, newly added or missed assets, newly added or missed service between current and previous scans, first scan or any specific scans performed previously.		
7.4	Shall support customization / editing of reports.		
7.5	Customized reports shall support creation of new templates and inclusion of customized logo and title.		
7.6	Shall be able to generate report based on scan groups (site), asset group (static or dynamic), and individual asset(s).		
7.7	Report shall be automatically generated after each complete scan or on a pre-determined frequency.		
7.8	Shall be able to export reports in various formats such as but not limited to CSV, PDF, RTF, HTML, Text and XML.		
7.9	Shall be able to export scan data in format such as but not limited to ARF, CSV, Cyber Scope XML, JDBC- Compliant Database, XML 1.0 and 2.0, SCAP XML, SQL Query Export and XCCDF.		

7.10	Shall be able to export scan data to external database for integration with external reporting system. Database Support shall include MSSQL, Oracle and MySQL.		
7.11	Shall include access controls to reports based on user roles.		
7.12	Shall be able to distribute reports to external recipient in the form of Electronic Mail (Email).		
7.13	Shall have the functionality to create dynamic groups by setting conditions including but not limited to asset name, asset risk score, CVSS, host type, IP range, Operating System (OS) name, PCI compliance status, service name, site name, software name and vulnerability type.		
7.14	System shall automatically categorize assets based on multiple attributes and create reports for these asset groups.		
7.15	Communicate executive findings, vulnerability trends and top vulnerabilities/assets to management in an easy to understand format		
7.16	Solution shall support aggregate scan data for consolidated reporting.		
7.17	Solution provide a single unified reporting interface for vulnerabilities, policy compliance and asset information.		
7.18	Solution support asset and vulnerability filtering by attributes, category, and severity.		
7.19	Solution shall automatically categorize assets based on multiple attributes and create reports for these asset groups.		
7.20	Solution support SQL queries to be run against the reporting data model.		
7.21	Solution support asset reporting by tags, sites, asset groups and assets and vulnerability filtering scoping by category, and severity.		
7.22	Library of drillable dashboards that display an integrated view of vulnerabilities, events and network activity		
8	Solution Requirements: Prioritization & Remediation		
8.1	Solution shall provide a granular risk score that takes into account malware/exploits exposure		
8.2	Solution shall prioritize remediation efforts for business- critical assets and risk score attached to it		
8.3	Solution shall built-in integration with a popular penetration testing tool (mention the tools name) for vulnerability validation.		
8.4	Solution shall allow integration of vulnerability validation results back into the solution for risk prioritization and management.		
8.5	Solution shall provide prioritized remediation plans that include IT operations level instructions based on the vulnerability filtering scoping		
8.6	Solution shall automatically assign remediation tasks after each scan according to the business context.		
9	Solution Requirements: Administration		
9.1	Solution shall support both pre-defined and custom role- based access		
9.2	Solution shall set permissions for functionality and sites/assets based on user		
9.3	Solution provide an approval workflow for vulnerability exceptions.		
9.4	Solution support configure user permissions for submission, approval and expiration based on roles		

9.5	Solution shall allow vulnerabilities exclusion should there be any identified exceptions and those exclusion will not appear in reports (unless time expiry applies)		
9.6	VA console shall include web-based user interface through encrypted channels.		
9.7	VA console shall include command line console.		
9.8	Shall support role-based customization on a per user basis to allow finer granular controls and/or extend/restrict permissions.		
9.9	Shall support external authentication system including but not limited to LDAP, AD and Kerberos.		
9.10	Shall include built-in diagnostic tools to display system status. Diagnostic tools shall be able to upload log files through encrypted channels for analysis.		
9.11	Shall be able to perform backup and restore of database, configuration files, and reports and scan logs.		
9.12	Receiving of updates shall be at least bi-weekly or more frequently.		
9.13	Solution support automatic, manual / offline updates.		
10	Solution Requirements: Installation, Deployment and Integration		
10.1	Software shall be able to install on Linux and Windows. It must be truly 64-bit architecture built		
10.2	Software shall officially support running on virtual and physical environment		
10.3	Shall provide distributed client/server architecture with unlimited scalability. A centralized management security console, which is able to manage multiple scan engines for consolidated reporting and data aggregation.		
10.4	Multiple scan engines shall be able to be grouped together to run any single scan to reduce and improve scanning time.		
10.6	Both the console and scanner engines shall be available on Software and Hardware appliances		
10.7	Software and OS of the appliance shall be true 64bit architecture and the OS shall be hardened.		
11	Solution Requirements: Licensing Model		
11.1	The vendor has to provide Annual Subscription license with three (3) years support from the date of License Delivery by OEM. Bank will start the service initially for 03 years. If the service of the solution is satisfactory, the bank may extend the subscription for next 02 years with the same price based upon the approval from the competent authority.		
12.	Delivery Partner: Minimum Requirement		
12.1	The local delivery partner must have minimum delivery experience of at least two (2) corporate clients in Bangladesh.		
12	Solution Requirements: Training		
12.1	Selected Provider/Vendor must ensure/conduct/arrange operation and maintenance training of respective procured product/tools for 10 -12 official of SIBL.		

Penetration Testing Tools/ Application

SL No.	Required Technical Specification		Bidders Response	Remarks
1	Solution Requirements: Solution Information			
1.1	Name of the Solution			
1.2	Version of Solution			
1.3	Name of the OEM			
1.4	Country of Origin			
1.5	No of User	01 (One) and must be able to launch penetration test to unlimited application/IP addresses		
2	Solution Requirements: Deployment			
2.1	What are the minimum and recommended system requirements to operate the solution?			
2.2	What is the average time for implementation?			
2.3	Has the solution been deployed by the local supplier in any organization in Bangladesh? Please mention at least two (2) client names where the solution was supplied directly by your organization.			
3	Solution Requirements: Interface			
3.1	The software must be windows-based software			
3.2	The software supports web-based interface allows users to optionally connect over HTTPS to utilize the product.			
3.3	The software must support wizard-based penetration test setup and configuration			
3.4	The software must support multi-stage attacks that pivot across systems, devices and applications using the windows-based GUI interface			
3.5	The software must support teaming feature whereby different testers have the capability to interact in the same workspace against the same environment across multiple copies of the software			
4	Solution Requirements: Network Penetration Testing			
4.1	The software must be able to gather network information and build system profiles			
4.2	The software must able to identify and exploit critical OS, device, service and application vulnerabilities			

4.3	The software must able to leverage compromised systems as beachheads to attack other network resources through VPN and proxy pivots		
4.4	The software must able to test defensive technologies' ability to identify and stop attacks		
4.5	The software must able to discover windows NTLM hashes and attempt to determine plaintext passwords for those hashes		
4.6	The software must able to discover identities including usernames, passwords, kerberos tickets/e-keys and SSH keys		
4.7	The software must able to utilize learned identities as part of multi-vector tests		
4.8	The software must able to leverage kerberos identities to launch attacks and find exposures		
4.9	The software must able to take control of systems via weak authentication manually or with the rapid penetration test wizard (RPT)		
4.10	The software must able to gain memory-based or persistent access to compromised systems by leveraging identity-based or exploit-based attacks		
4.11	<p>The software must able to import results from multiple network vulnerability scanners and validate the results for exploitability. These scanners include:</p> <ul style="list-style-type: none"> + Beyond Security AVDS + GFI LANguardTM + IBM Enterprise Scanner + IBM Internet Scanner + McAfee Vulnerability Manager + Tenable Nessus + Rapid7 Nexpose + Patchlink VMS + NMap + QualysGuard + Retina Network Security Scanner + SAINTscanner + TripWire IP360 		
4.12	The software must able to support remediation validation function to re-test vulnerabilities found within a workspace for remediation verification		
4.13	The software must support REST API		
4.14	The software must able to support remediation validation function to re-test vulnerabilities found within a workspace for remediation verification		
5	Solution Requirements: Web Application Penetration Testing		
5.1	The software must able to identify weaknesses in web applications, web servers and associated databases		
5.2	The software must able to test for all latest OWASP Top Ten Web Application vulnerabilities		
5.3	The software must able to dynamically generate exploits that can compromise security weaknesses in custom applications		

5.4	The software must able to import and validate results from web vulnerability scanners to confirm exploitability and prioritize remediation. The web vulnerability scanners include: + Qualys Web Application Sanner + Portswigger BurpSuite Professional + Trustwave AppScan + HP WebInspect + IBM Security AppScan + Rapid7 AppSpider + Acunetix® Web Security Scanner		
5.5	The software must able to support pivot attacks to the web server and backend network		
5.6	The software must able to support web services testing for web and mobile applications		
6	Solution Requirements: Client-Side Penetration Testing		
6.1	The software must able to crawl sites, search engines, etc. for target emails information		
6.2	The software must able to sit between tested users and real websites capturing exchange of information		
6.3	The software must able to auto-tag users failing for phishing techniques for easy re-testing		
6.4	The software must able to leverage a variety of templates or create custom phishing emails		
6.5	The software must able to use client-side exploits to test endpoint system security, access defenses and pivot to network penetration test		
7	Solution Requirements: Wireless Network Penetration Testing		
7.1	The solution must include capabilities for discovering and analyzing wireless networks.		
7.2	The solution must assess the exploitability of networks encrypted with WEP, WPA and WPA-2.		
7.3	The solution must be able to replicate wireless man in the middle attacks.		
7.4	The solution must be able to detect systems probing for SSIDs.		
7.5	The solution must be able to impersonate SSIDs (karma).		
7.6	Please mention if any additional hardware/wireless networking auditing tool is required to create a Fake Access Point for wireless network testing.		

8	Solution Requirements: Mobile Device Penetration Testing		
8.1	The solution must include capabilities for demonstrating the exploitability of smartphones. Please summarize the solution's smartphone testing capabilities, including target mobile platforms.		
8.2	The solution must offer multiple smart phone attack replication capabilities. Please describe each mobile device attack capability.		
8.3	The solution must demonstrate exploitability through evidence retrieval capabilities. Please describe all evidence retrieval capabilities included in the solution.		
8.4	The solution must allow use to interact with the compromised device.		
9	Solution Requirements: Reporting		
9.1	The software must able support comprehensive and customizable reporting capabilities		
9.2	The software must include the following report data and is also able to export the data in Crystal Report, Spreadsheet and PDF report format: <ul style="list-style-type: none"> • CVE numbers • CVSS ratings 		
10	Solution Requirements: Software License		
10.1	Must be able to scan multiple IP addresses concurrently in a single workspace		
10.2	Must be included with stable, up-to-date library of commercial- grade exploits. The vendor has to provide Annual Subscription license with three (3) years support from the date of License Delivery by OEM. Bank will start the service initially for 03 years. If the service of the solution is satisfactory, the bank may extend the subscription for next 02 years with the same price.		
11	Delivery Partner: Minimum Requirement		
11.1	The local delivery partner must have minimum delivery experience to at least two (2) clients in Bangladesh Banking sector of the offered solution.		
12	Solution Requirements: Training		
12.1	Selected Provider/Vendor must ensure/conduct/arrange operation and maintenance training of respective procured product/tools for 10 -12 official of SIBL.		

Web Application Scanning Tool

SL No.	Required Technical Specification		Bidders Response	Remarks
1	Solution Requirements: Solution Information			
1.1	Name of the Solution			
1.2	Version of Solution			
1.3	Name of the OEM			
1.4	Country of Origin			
1.5	No of User	01 (One) and must be able to scan unlimited web application		
2	Solution Requirements: Technical Feature			
2.1	Solution shall provide complete, accurate, and scalable web security and enables organizations to assess, track, and remediate web application vulnerabilities.			
2.2	Solution shall include web application scanning capabilities against web technologies including but not limited to AJAX, ASP.NET 2.0 and Flash-based sites.			
2.3	Solution must provide automated crawling and testing of custom web applications to identify vulnerabilities including Cross-site scripting (XSS) and SQL injection.			
2.4	Solution shall be able to Detect, identify, assess, track and remediate latest OWASP Top 10 risks, WASC threats, CWE Weaknesses, and web application CVEs.			
2.5	Solution shall support credential login through HTTP Form and Basic Digest authentication for scanning.			
2.6	Solution shall have maximum scan coverage, including advanced scripting and the open source browser automation system for web app testing			
2.7	Solution shall support web spidering/crawling to gather security related information such as directory structures, files and applications running on the web servers.			
2.8	Solution shall have the functionality to set scan rate such as thread per web server and spider request delay to control bandwidth consumption and scanning time.			
2.9	Solution shall have the functionality to exclude scan by HTTP daemon and path.			
2.10	Solution shall have large vulnerability database to check.			
2.11	Solution Should be able to Identify and report malware present in websites and apps			
2.12	Solution should support Immediate deployment – no hardware to set up, always up to date			
2.13	Solution should provide Centralized management – to be able to apply policies consistently across application			

2.14	Solution should be able to Consolidate automated scan data from WAS with data from manual testing approaches, to get a complete view of your web app vulnerabilities.		
2.15	Solution should be able to Prioritize remediation and focus on the most critical flaws		
2.16	Solution should suggest remediation actions for the identified weaknesses		
2.17	Solution should allow to check status of the scan in real time		
2.18	Solution should be able to perform incremental scans (i.e., scan only the delta of a previously scanned application)		
2.19	Solutions should provide Unified, interactive dashboard lets one understands the security of web applications at a glance.		
2.20	Solution should allow automated dynamic deep scanning to quickly get visibility of the vulnerability. It should have the features of Application discovery and cataloging – to find new and unknown web applications in the network.		
2.21	Solution Should be able to insert security into application development and deployment in DevSecOps environments. detect code security issues early and often, test for quality assurance and generate comprehensive reports. Support for robust API and a native plugin, it should provide everything need to automate scanning in CI/CD environment.		
2.22	Solution should be able to scan websites, and identifies alerts to infections, including zero-day threats via behavioral analysis. Detailed malware infection reports accompany infected code for remediation.		
2.23	Solution shall have option to integrate with Web Application Firewall to virtually patch with blocking rules, providing developers with time for code repair.		
2.24	Solution must be already delivered in at least 3 (Three) organizations in Bangladesh by the local solution provider/ bidder		
3	Solution Requirements: Licensing Model		
3.1	License to be provided for Minimum 1(One) Web Application- Automated web application scanning vulnerabilities.		
3.2	The vendor has to provide Annual Subscription license with three (3) years support from the date of License Delivery by OEM. Bank will start the service initially for 03 years. If the service of the solution is satisfactory, the bank may extend the subscription for next 02 years with the same price.		
4	Delivery Partner: Minimum Requirement		
4.1	The local delivery partner must have minimum delivery experience to at least two (2) clients in Bangladesh Banking/Financial sector of the offered solution.		
5	Solution Requirements: Training		
5.1	Selected Provider/Vendor must ensure/conduct/arrange operation and maintenance training of respective procured product/tools for 10 -12 official of SIBL.		

INVITATION FOR TENDER
PROCURING VAPT & WEB SCANNING TOOLS

Bidder Reg. No.
Tender Ref. SIBL/HO/LSD/2023/725
Date:11/05/2023

Registration close date:08/06/2023
Tender Submission Date: 11/06/2023

Section D: Price Quotation & Contact information

Items	Price (1 st year)	Price (2 nd year)	Price (3 rd Year)	Price for 3 years
Item 1: Vulnerability Management tools with con/warranty/support and services/subscription				
Item 2: Penetration Testing tools with con/warranty/support and services/subscription				
Item 3: Web Application Scanning tools with con/warranty/support and services/subscription				
Training Cost (if any) for above items				
Grand Total Price				

Grand Total price (in words):

(The bank will pay VAT only as per rule of the government of Bangladesh)

Signature & Seal of the bidder :
Name of the Bidder :
Designation of the Bidder :
Company Name :
Business Address :
Contact email address :
Mobile No. :