FSIB
ISLAMI BANK

First Security Islami Bank Limited
ICT Division

Head Office
Plot#12, 2nd & 3rd Floor, Main Road.
Block # A, P.S- Badda,
Bashundhara R/A, Dhaka-1229.
Web: www.fsiblbd.com; email: ict@fsiblbd.com

Ref: FSIBL/HO/ICT/0229/2022 Date: 13.04.2022

REQUEST FOR PROPOSAL (RFP)

For Purchasing Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center.

Bidder Reg. No.

Section A: General Information

<table>
<tr><th>SN</th><th colspan="2">Item</th><th colspan="7">Description</th></tr>
<tr><td>1</td><td colspan="2"><b>Name of the Bank</b></td><td colspan="7"><b>First Security Islami Bank Limited</b></td></tr>
<tr><td>2</td><td colspan="2"><b>Procuring Entity Name</b></td><td colspan="7">Information & Communication Technology Division</td></tr>
<tr><td>3</td><td colspan="2"><b>Invitation of tender for</b></td><td colspan="7">Supply & implementation of Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center as per technical specifications detailed in "Section C & D" hereunder from the eligible Partners as specified in "Section B" hereunder.</td></tr>
<tr><td>4</td><td colspan="2"><b>Invitation for Quotation Ref. & Date</b></td><td colspan="7">FSIBL/HO/ICT/229/2022 Date: 13.04.2022</td></tr>
<tr><td>5</td><td colspan="2"><b>Procurement Method</b></td><td colspan="7">Open Tendering Method</td></tr>
<tr><td>6</td><td colspan="2"><b>Source of Fund</b></td><td colspan="7"><b>First Security Islami Bank Limited</b></td></tr>
<tr><td>7</td><td colspan="2"><b>Registration of bidders & price of Tender Document:</b></td><td colspan="7">The interested eligible bidders have to enroll their name by submitting a prayer along with a non-refundable registration/enrollment fee <b>Tk.2,500.00 (Taka Two Thousand Five Hundred)</b> only in the form of "Payment Order" in favor of "<b>First Security Islami Bank Limited</b> during submission of tender. No Tender documents will be sold physically. The bidder have to copy or download this tender documents from the website: www.fsiblbd.com and place them on their own letterhead to submit their bid.</td></tr>
<tr><td rowspan="4">8</td><td rowspan="4"><b>Tender Process Dates & Times</b></td><td><b>Tender</b></td><td colspan="2"><b>Registration</b></td><td colspan="2"><b>Pre-Bid Meeting</b></td><td colspan="2"><b>Submission</b></td><td><b>Opening Time</b></td></tr>
<tr><td><b>Process</b></td><td><b>Start</b></td><td><b>End</b></td><td colspan="2"></td><td><b>Start</b></td><td><b>End</b></td><td></td></tr>
<tr><td><b>Date</b></td><td>13.04.2022</td><td>28.04.2022</td><td colspan="2">19.04.2022</td><td>28.04.2022</td><td>28.04.2022</td><td>28.04.2022</td></tr>
<tr><td><b>Time</b></td><td>10.30 AM</td><td>02:00 PM</td><td colspan="2">11.00 AM</td><td>10:00 AM</td><td>03:00 PM</td><td>03:20 PM</td></tr>
<tr><td>9</td><td colspan="2"><b>Place of opening and receiving tender documents</b></td><td colspan="7"><b>First Security Islami Bank Limited</b>, Plot#12, 3rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.</td></tr>
<tr><td>10</td><td colspan="2"><b>Composition of bid Price shall be inclusive of</b></td><td colspan="7">The costs of complete Purchasing Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools as instructed by the bank, testing, commissioning, delivering to directed site 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.</td></tr>
<tr><td>11</td><td colspan="2"><b>Awarding the successful bidder</b></td><td colspan="7">The bank may negotiate with the successful bidder or all bidders regarding price reduction modification if necessary before issuing the acceptance letter. A notification of award (NOA) will be provided by Bank to the successful bidder. Within 07 days of receipt of the Letter of Acceptance, the successful bidder shall sign a copy of it and return to the bank. Work must be completed within the time specified in the Work Order/Contract.</td></tr>
<tr><td>12</td><td colspan="2"><b>Payment & Security</b></td><td colspan="7">The bidder shall furnish as bid security of 2.50% of the total financial offer in the form of bank draft or bank guarantee in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The bid security shall be submitted along with the tender inside the envelop marked as "Financial Offer- for <b>Purchasing Vulnerability Assessment tools, Penetration</b></td></tr>
</table>

First Security Islami Bank Ltd.
FSIB ISLAMI BANK
ICT Division
Head Office, Dhaka

		Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center" The bid security should be valid for 60 days after the date of bid opening. Any bid not accompanied by an acceptable bid security shall be rejected as non-responsive. The bid security of unsuccessful bidders will be returned within 7 days from the date awarding the successful bidder. The bid security of the successful bidder will be returned when the bidder has signed the NOA and furnished the required performance security. The bid security may be forfeited if (a) the bidder withdraws its bid during the period of bid validity specified in the bid form; (b) if a successful bidder fails to sign the contract and (c) if a successful bidder fails to furnish the performance security.
		Within 07 days of receipt of the notification of award from the Bank, the successful bidder shall furnish as performance security of 10% of total amount in the form of pay order or bank guarantee from any scheduled bank in favor of First Security Islami Bank Limited. The performance security should be valid till the successful competition of the project including products delivery & service integration to its full extent.
		Bid shall remain valid for a period of 3 (Three) months after the date of opening of the proposals. In exceptional circumstances, prior to expiry of the original bid validity period, the Bank may request the bidder to extend the period of validity for a specified additional period. The request and the responses shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.
		50% payment of total price may be provided as an advance payment upon request of the successful bidder. 50% payment may made after implementation of Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools licenses in its environment for DC & DR upon getting satisfactory certificate from ICT Division, FSIBL, Head Office expressing clearly that the end user has no objection.
		In case of a failure of the successful Bidder to provided Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools with license in the prescribed time, the bidder will be liable to pay 0.5% of the Contract price as liquidated damages for every week after the deadline and will be deducted from the bill amount. The maximum penalty will be 10% of total contact price.
13	**Submission of bidders Qualifications/Eligibility 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 a separate sealed envelope with proper labeling mentioning- "Bidder's Qualifications /Eligibility for supplying & implementation of Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools" license, Name of the bidder & Registration No.
14	**Submission of Technical & Financial Offer**	The interested registered bidder shall copy the Asked Technical Specifications and Financial Offer form from the webpage and place them on their own letterhead and write their price offer for Section "C"" in the designated field(s) and submit the document in a separate sealed envelope with proper labeling mentioning- "Financial Offer- for Purchasing Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center", Name of the bidder & Registration No.
15	**Name and address of the Office for receiving tender(s)**	Vice President & Head of ICT Division. First Security Islami Bank Limited, Plot#12, 3rd Floor, Main Road. Block # A, P.S- Badda, Bashundhara R/A, Dhaka-1229.
16	**Address of Official Inviting Tender**	Do.
17	**Contact Details**	Telephone No. 02-8432613-22 Ext: 302,304 email: ict@fsiblbd.com
18	**Special Instruction**	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 7. Bidder have to bid full of the Section "C" & "D" 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.

First Security Islami Bank Ltd.
FSIB
ICT
Division
Head Office, Dhaka

REQUEST FOR PROPOSAL (RFP)

For Purchasing Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center

Tender Ref: FSIBL/HO/ICT/0229/2022
Date: 13.04.2022
Bidder Reg. No.

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** [Proprietorship, Partnership, Private Limited, Public Limited etc.]	Required		
05	**Website address of the company**	Required		
06	**Bidder's Office Phone No.**	Required		Attach bill copy
07	**Bidder's email address**	Required		Send "Test" mail to ict@fsiblbd.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 "Test" mail to ict@fsiblbd.com
13	**Valid Trade License No.**	Required		Attach proof
14	**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	**Bank solvency certificate**	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 3 (Three) years of experience for supplying similar Solutions or Services.**	Experience / Work Completion Certificate		Attach proof
21	**Are you Banned by any bank authority or? Government agency?**	Yes/No		

Statement of the bidder: All the above information provided here in above 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.

First Security Islami Bank Ltd. ★ Head Office, Dhaka ★
FSIB
ICT Division

REQUEST FOR PROPOSAL (RFP)

For Purchasing Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools at Data Center

Tender Ref: FSIBL/HO/ICT/0229/2022
Date: 13.04.2022
Bidder Reg. No

Section C: Technical/Financial Specifications of Vulnerability Assessment tools, Penetration Testing Tools, Web Application Scanning Tools and Application Security Testing Tools

1. **Common Vulnerability Assessment and Management Tools (Including PCI Internal Vulnerability Scanning):**

SL no.	Required Technical Specification		Bidders Response	
			Complaint (Y/N)	Remarks
1	**Solution Requirements: 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	2000		
1.5	Deployment Type	On Premise		
2	**Market Recognition**			
2.1	Proposed solution must be recognized as Leader in the last published report by Forrester Wave for VM.			
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 off 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.)			

First Security Islami Bank Ltd.
FSIB
ICT Division
Head Office, Dhaka

Signature & Seal of the bidder

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 Agentless (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 must include active and passive scanning Capability for full visibility of vulnerability and configuration.		
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 STIGSsecurity 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 Ssecurity 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.		

Signature & Seal of the bidder

First Security Islami Bank Ltd. ★ Head Office, Dhaka ★
FSIB ISLAMI BANK
ICT Division

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 shallintegrate with Cisco FireSIGHT Management Center.		
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, and others)		
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		
	Send events to enterprise SIEM systems		
7	Solution Requirements: Reporting		
7.1	Remediation reports shall provide step-by-step guide foradministrators to fix the vulnerabilities found. It shall alsoinclude 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, topremediation, 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 newtemplates 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 eachcomplete scan or on a pre-determined frequency.		
7.8	Shall be able to export reports in various formats suchas but not limited to CSV, PDF, RTF, HTML, Text and XML.		
7.9	Shall be able to export scan data in format such as butnot 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 recipientin the form of Electronic Mail (Email).		
7.13	Shall have the functionality to create dynamic groups bysetting 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 andvulnerability type.		
7.14	System shall automatically categorize assets based on multiple attributes and create reports for these assetgroups.		
7.15	Communicate executive findings, vulnerability trends and top vulnerabilities/assets to management in an easy to understand format		

First Security Islami Bank Ltd.
★ Head Office, Dhaka ★
FSIB ISLAMI BANK
ICT Division

Signature & Seal of the bidder

7.16	Solution shall support aggregate scan data forconsolidated 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 byattributes, category, and severity.		
7.19	Solution shall automatically categorize assets based onmultiple attributes and create reports for these asset groups.		
7.20	Solution support SQL queries to be run against thereporting data model.		
7.21	Solution support asset reporting by tags, sites, assetgroups and assets and vulnerability filtering scoping by category, and severity.		
7.22	Library of drillable dashboards that display an integratedview of vulnerabilities, events and network activity		
8	**Solution Requirements: Prioritization & Remediation**		
8.1	Solution shall provide a granular risk score that takes intoaccount 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 popularpenetration 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 andmanagement.		
8.5	Solution shall provide prioritized remediation plans that include IT operations level instructions based on thevulnerability filtering scoping		
8.6	Solution shall automatically assign remediation tasksafter 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 andsites/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 interfacethrough encrypted channels.		
9.7	VA console shall include command line console.		
9.8	Shall support role-based customization on a per userbasis to allow finer granular controls and/or extend/restrict permissions.		
9.9	Shall support external authentication system includingbut not limited to LDAP, AD and Kerberos.		
9.10	Shall include built-in diagnostic tools to display systemstatus. 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 morefrequently.		
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. Itmust be truly 64-bit architecture built		
10.2	Software shall officially support running on virtual andphysical environment		
10.3	Shall provide distributed client/server architecture with unlimited scalability. A centralized management securityconsole, which is able to manage multiple scan engines for consolidated reporting and data aggregation.		

Signature & Seal of the bidder

First Security Islami Bank Ltd.
FSIB ISLAMI BANK
ICT Division
Head Office, Dhaka

10.4	Multiple scan engines shall be able to be groupedtogether to run any single scan to reduce and improve scanning time.		
10.6	Both the console and scanner engines shall be availableon Software and Hardware appliances		
10.7	Software and OS of the appliance shall be true 64bitarchitecture and the OS shall be hardened.		
11	**Solution Requirements: Licensing Model**		
11.1	License to be provided for Minimum 2000 IP's		
11.2	The vendor has to provide Annual Subscription license with three (3) years support from the date of LicenseDelivery by OEM.		
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 where, at least one client must be running VM solution covering Minimum 2000 IP or more .		

2. Web Application Scanning (DAST):

SL No.	Required Technical Specification	Bidder Response	
		Complaint (Y/N)	Remarks
1.0	**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 (Country of origin must be North America / Europe region)		
2.0	**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 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		
	Solution should support Immediate deployment – no hardware to set up,		

First Security Islami Bank Ltd. ★ Head Office, Dhaka ★
ICT Division

2.12	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		
3.0	**Solution Requirements: Licensing Model**		
3.1	License to be provided for Minimum 1(One) Web Application- Automated web application scanning for SQL injection and XSS vulnerabilities.		
3.2	The vendor has to provide Annual Subscription license with three (3) years support from the date of License Delivery by OEM.		

3. Common Penetration Testing Tools/ Application (Including Network Rpt. Client Rpt, Web Rpt):

SL No.	Required Technical Specification	Bidder Response	
		Complaint (Y/N)	Remarks
1.0	**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 (Country of origin must be North America / Europe region)		
2.0	**Solution Requirements: Deployment**		

First Security Islami Bank Ltd.
FSIB ISLAMI BANK
ICT Division
★ Head Office, Dhaka ★

Signature & Seal of the bidder

2.1	What are the minimum and recommended system requirements to operate the solution?		
1.2	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.		
3.0	**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		
4.0	**Solution Requirements: Network Penetration Testing**		
4.1	The software must 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	The software must able to import results from multiple network vulnerability scanners and validate the results for exploitability. These scanners include: + Beyond Security AVDS + GFI LANguardTM + IBM Enterprise Scanner + IBM Internet Scanner + McAfee Vulnerability Manager		

First Security Islami Bank Ltd.
FSIB
ICT Division
Head Office, Dhaka

Signature & Seal of the bidder

	+ 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		
4.25	The software must able to support remediation validation function to re-test vulnerabilities found within a workspace for remediation verification		
5.0	**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 OWASP Top Ten 2017 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		
6.0	**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		
7.0	**Solution Requirements: Wireless Network Penetration**		

Signature & Seal of the bidder

First Security Islami Bank Ltd.
FSIB
ISLAMI BANK
ICT Division
Head Office, Dhaka

	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.		
8.0	**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.		
9.0	**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: • CVE numbers • CVSS ratings		
10.0	**Solution Requirements: Software License**		
10.1	Must be able to scan 8IP concurrently in a single workspace		
10.2	Must be included with stable, up-to-date library of commercial- grade exploits		
11.0	**Delivery Partner: Minimum Requirement**		
11.1	The local delivery partner must have minimum delivery experience to at least two (2) corporate clients in Bangladesh of the offered solution.		

4. Application Security Testing Tool:

SL No.	Required Technical Specification	Bidder Response	
		Complaint (Y/N)	Remarks
1.0	**Solution Requirements: Product Information**		
1.1	Name of the Product		
1.2	Version		
1.3	Name of the OEM		

First Security Islami Bank Ltd.
ICT Division
Head Office, Dhaka

Signature & Seal of the bidder

1.4	Country of Origin (Country of origin must be North America / Europe region)		
2.0	**Solution Requirements: Basic Functionality**		
2.1	The Solution should provide Automated Source Code Security Review		
2.2	The solution must provide vulnerability explanation and fix recommendations during the vulnerability remediation process, including line-of-code details and descriptions on how to remediate each vulnerability and in the correct programming language.		
2.3	The solution should provide accurate result and detect a breadth of issues, prioritizing vulnerabilities to provide a detailed and accurate action plan, delivering risk ranked and categorized issues		
2.4	Ability to identify risks in all types of applications such as in-house, outsource, third party, open source and/or mobile applications etc.		
2.5	Support scanning of mobile-based applications for Android, iOS, Windows, Android, iOS and Hybrid mobile applications		
2.6	Aggregate and correlate assessment results for enhanced reporting of vulnerabilities		
2.7	The scanning should be Centralized & user machines should not require heavy resources		
2.8	Ability to mark false positive vulnerabilities and false negative		
2.9	The solution must be able to scan the multiple codes in parallel.		
2.10	The solution must be agent less and should be able to communicate with the Code Servers/ Repositories		
2.11	The solution should have capability of Full and incremental code scanning		
2.12	The solution should have capability of Code Analysis for Zero-Tolerance Defect Environments		
3.0	**Solution Requirements: Programming Languages & Frameworks**		
3.1	The solution should support wide range of programming languages including languages like: Java, J2SE, J2EE, JSP, C#, VB.NET, JavaScript, NodeJs, VBScript, PL\SQL, HTML 5, ASP, VB6, C/C++, PHP, Ruby, Perl and Python		
3.2	The solution must support scanning of mobile-based applications for Android, iOS, Windows and Hybrid mobile applications.		
3.3	The solution must support wide variety of development environments, platforms, and frameworks to enable security reviews for both Web and Mobile platforms.		
3.4	The solution must not require any configuration while scanning and should recognize all supported programming languages automatically, scan them for security vulnerabilities and gives single aggregated report for all the technologies scanned.		
3.5	The solution should support scanning of all types of custom code, libraries, frameworks and runtime platform		
4.0	**Solution Requirements: Scan Methodology**		
4.1	The Source Code Security Analyzer shall have a client Web browser-based user interface to scan, results, etc.		

First Security Islami Bank Ltd.
FSIB ISLAMI BANK
ICT Division
Head Office, Dhaka

Signature & Seal of the bidder

4.2	The Source Code Security Analyzer shall be agnostic to compilers such that the same tool will be used for scanning code anywhere regardless of the Operating System or Development Environment.		
4.3	The scanning should be centralized and user machines should not require heavy resources.		
4.4	The solution should support automated closure of vulnerability on rescan if resolved.		
4.5	The solution should have ability to schedule the code scan activity.		
4.6	The solution should support delta or incremental scan		
5.0	**Solution Requirements: Weaknesses Detection Rules**		
5.1	The Source Code Security Analyzer shall come pre-configured with hundreds of known security vulnerabilities for multiple programming languages.		
5.2	The Source Code Security Analyzer shall have out-of-the-box support for satisfying the following regulations: PCI, OWASP Top 10 and CWE/SANS Top 25.		
5.3	The Source Code Security Analyzer shall have an open architecture that will allow to modify, customize existing rules and create new rules.		
6.0	**Solution Requirements: Scan Results**		
6.1	The Source Code Security Analyzer shall be capable, at the completion of a vulnerabilities scan, of producing reports that include: Issues found in the scanned code, Recommendations of how to fix the found issues, categorization of found issues by type and severity.		
6.2	The solution should have ability to mark false positive vulnerabilities and false negative and remember them in subsequent scans, in order to reduce False Positive results		
6.3	It shall be possible to modify reporting templates and select which details will be produced.		
6.4	The Source Code Security Analyzer shall allow the inclusion of comments in the vulnerabilities identified during a scan to record user feedback.		
6.5	The Source Code Security Analyzer shall display unidentified vulnerabilities according to severity categories – High Risk, Medium Risk, Low Risk or Info. It should be possible to modify the default Classification categories.		
6.6	The Source Code Security Analyzer shall allow to compare the results of several scans while clearly indicating the differences as trend graphs. The reports shall clearly indicate new issues, resolved issues, and recurring issues.		
6.7	The Source Code Security Analyzer will support table presentation and graphical presentation of detected vulnerabilities.		
6.8	The Source Code Security Analyzer shall be able to display the results in a graphical presentation that clearly illustrate data flows throughout the application and pinpoint common nodes where multiple attack vectors converge, thus indicate best fix locations of multiple vulnerabilities with one fix.		
6.9	The solution must fulfil the functional requirements set by NIST		
6.10	The solution must fulfil the functional requirements set by PCI		
7.0	**Solution Requirements: Dashboard & Implementation**		

First Security Islami Bank Ltd.
FSIB ISLAMI BANK
ICT Division
Head Office, Dhaka

Signature & Seal of the bidder

7.1	The Source Code Security Analyzer shall have a dashboard display that will present various project scanning metrics facilitating to determine priorities and management decisions.		
7.2	The Source Code Security Analyzer Implementation should be 100% on premise and shall be installed on a server housed in an internal network		
7.3	Types of vulnerabilities it can detect (out of the OWASP Top Ten?) (plus, more?) Mention Your Offering.		
7.4	What is the accuracy Rate? False Positive/False Negative rates? Does the tool have an OWASP Benchmark score?		
7.5	Solution Must be able to scan Partial Code. So, the developer will have the ability to run a scan during his work without the need to wait for the completion of his development task.		
7.6	The Solution Must be able to integrate with the developer's IDE (Visual Studio, Eclipse and so more.)		
7.7	The Proposed solution Must be Certified on • ISO.IEC 27001.2018_IL &ISO.IEC 27001.2018_USA • SOC 2 Type II.		
8.0	**Solution Requirements: Reporting**		
8.1	Provide flexible, detailed security issues reports that enable users to group and organize report data in multiple ways		
8.2	Support security compliance reports including standards including PCI Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS).		
8.3	Solution shall support report template customization from default available ones.		
8.4	Customized reports shall allow creation of new templates and inclusion of customized logo and title.		
8.5	Solution shall have flexible report generation capabilities (e.g. User wise, Application wise, Module wise, group wise etc.)		
8.6	Solution shall support report scheduling capabilities. Application should be able to automatically send reports when scans are completed.		
8.7	Solution shall be able to export reports in various formats		
8.8	Solution shall be able to generate report based on change management (duration / event)		
9.	**Solution Requirements: Compliance Status**		
9.1	Solution shall include built-in compliance checks		
9.2	Ability to provide for compliance with requirement set by like CIS, CWE/SANS, OWASP, PCI etc.		
9.3	Solution shall be able to check configuration based on inbuilt template and customized bench mark (e.g. Bangladesh Bank)		
9.4	Ability map scan results to compliance standards.		
10	**Solution Requirements: Licensing Model**		
10.1	License must be able to support minimum 10 projects, where projects are defined as a project may be used to (continuously) scan a single codebase which is maintained over time. The codebase is typically used to build a particular named software module or application.		

Signature & Seal of the bidder

First Security Islami Bank Ltd.
FSIB
ICT Division
Head Office, Dhaka

11.	**Solution Requirements: Issue Tracking**		
11.1	Provide built-in issue management capabilities and integration with development and quality assurance systems		
12.0	**Delivery Partner: Minimum Requirement**		
12.1	The local delivery partner must have minimum delivery experience to at least Two (2) corporate clients in Bangladesh of the offered solution.		

Section D: User Training

Requirements		Quoted Specification	Remarks
1.	In-person Installation and Administration training. The vendor / supplier must provide adequate and appropriate training to at least 10 bank personnel for an efficient operation of the System at Dhaka by an OEM certified trainer.		
2.	The local bidder shall provide Training registration for at least two (2) persons to access and exam voucher to any internationally recognize and Accredited Training Course on Penetration Testing.		
3.	Separate training has to be provided for the tools		
4.	A detailed training plan with specifications for Training courses, schedules, site and requirements must defined.		
5.	The trainer should have at least two years of expertise and delivered training on the specific domain on which training is being delivered.		
6.	Training documentation have to be provided.		

** The above mentioned price is inclusive of all costs, taxes & VATs as per rule of the government of Bangladesh.

Name of the Bidder :
Designation of the Bidder :
Company Name :
Business Address :
Mobile No. :

First Security Islami Bank Ltd.
FSIB
ICT Division
★ Head Office, Dhaka ★

Signature & Seal of the bidder