ISLAMI BANK BANGLADESH LIMITED
OPERATIONS WING, ENGINEERING DIVISION,
Procurement of Computer Hardware and Accessories Department,
Head Office, Yousuf Chamber (9th Floor),
20, Dilkusha C/A, Dhaka – 1000

Ref: IBBL/HO/ED/PCHAD/ **Dated: 31.07.2018**

NOTICE: Inviting Tender for procurement of Software Source Code Review Solution for IBBL.

Sealed Tenders are hereby invited by Islami Bank Bangladesh Limited from reputed Companies/ Manufacturers/ Local Agents/ Firms/ Suppliers & Installers of internationally reputed /Branded solution providers for supply, installation, configuration, testing, Training and implementation of **Software Source Code Review Solution for** IBBL. Brief description of the solution is as under:

Name & Description of the required solutions:

SL	Item description	Item Details
1	Source Code Review Tools	1 User License

Specifications of the Item:

Item	Requirement	Bidder Response
1.	**Functional Requirements**	
	Programming Languages & Frameworks: **a)** The solution must 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, Apex, Ruby, Perl, Python and Go,IONIC, Phonegap. **b)** The solution must support scanning of mobile-based applications for Android, iOS, Windows and Hybrid mobile applications. **c)** The solution must support wide variety of development environments, platforms, and frameworks to enable security reviews for both Web and Mobile platforms. **d)** The solution should recognize different programming languages, scan each language and combine the results into a single aggregated report **e)** The solution must understand frameworks like Spring, JSP, Hibernate, AngularJS and Angular2.	
2.	Scan Methodology	
	a) The SAST (Static Application Security Testing) shall have a client Web browser based user interface to manage projects, scans, results, etc. b) The SAST (Static Application Security Testing)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. c) The SAST (Static Application Security Testing)shall be able to scan source code which is incomplete and non-functional at various stages throughout the development cycle, before compilation and builds. d) The SAST(Static Application Security Testing) shall support	

	Command Line Interface (CLI) in order to: Allow to create new projects, allow to append a new scan to an already existing project, integrating with scheduling tools. e) The scanning should be centralized & user machines should not require heavy resources. f) The solution should support automated closure of vulnerability on rescan if resolved. g) The solution should have ability to schedule the code scan activity. h) The solution should support delta or incremental scan	
3.	a) The SAST (Static Application Security Testing)shall come pre-configured with hundreds of known security vulnerabilities for multiple programming languages. b) The SAST (Static Application Security Testing)shall have out-of-the-box support for satisfying the following regulations: PCI, HIPAA, OWASP Top 10, CWE/SANS Top 25, JSSEC, MISRA-C, MISRA-C++ c) The SAST (Static Application Security Testing)shall have an open architecture that will allow to modify, customize existing rules and create new rules. d) The SAST (Static Application Security Testing)shall be flexible to allow the customization of new rules in a visual manner without requiring coding or scripting. It should be possible to customize new rules according to the criticality of the vulnerability detected by them.	
4.	Integrations	
	a) The SAST (Static Application Security Testing)will support integration at different stages of application life-cycle. In particular: Development Environment Plugins, Source Code Repositories, Build Management Tools, Issues/Bugs Tracking Systems. b) **The SAST must have have out-of-the-box integration with the following IDEs: Eclipse, Visual Studio and Intellij Idea**. c) The SAST shall have out-of-the-box integration with the following QA tools: Sonar, TFS and Jira. d) The SAST shall have out-of-the-box integration with the following Build Systems: Jenkins, Bamboo. e) The SAST shall have out-of-the-box integration with the following Source Control Repositories: TFS, GIT, CVS,SVN and Perforce. f) The SAST shall have an API for allowing developers to create client scripts that work with scanning projects, scan results and reports.	
5.	**Scan Results**	
	a) The SAST 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, A categorization of found issues by type and severity. b) 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 c) It shall be possible to modify reporting templates and select which details will be produced.	

	d) The SAST shall allow the inclusion of comments in the vulnerabilities identified during a scan to record user feedback. e) The SAST 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. f) The SAST shall allow to export scan results in the following formats: PDF, RTF, CSV and standard XML format for possible integrations with SIEM systems. g) The SAST 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. h) The SAST will support table presentation and graphical presentation of detected vulnerabilities. i) The SAST 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. j) The SAST shall allow the automatic sending of scan results in PDF/Excel to a selected email address. k) The solution should provide its OWSAP Benchmark score, and provide false positive/false negative rate.	
6.	**Dashboard**	
	a) The SAST shall have a dashboard display that will present various project scanning metrics facilitating to determine priorities and management decisions. b) The Dashboard presentation will be configurable to display different views to different users, according to their authorization levels.	
7.	**Implementation**	
	a) The SAST shall be scalable to support various organization sizes and loads. b) The SAST Implementation should be 100% on premise. c) The SAST shall support a distributed architecture, whereas multiple / parallel scans should be possible. **Hardware** d) The SAST shall allow vertical scalability of hardware withouthaving to perform changes to hosted application. e) The SAST shall support horizontal scalability of hardware by deploying cluster configuration with load balancing that do not require 3rd party external software solutions.	
8.	**Users and teams**	

	a) The SAST shall allow system administrators to define different users' groups in teams, sub-teams and organizations within the company. b) Team members shall have different actions and visibility permissions according to their role association. c) The SAST shall allow system administrators to define an organization structure. The hierarchy shall be displayed in a clear graphical tree illustration. d) Only authorized users shall be able to initiate scans. e) Team members will have access only to their own team's reports.	

**SAST= (Static Application Security Testing)

Terms and Conditions

01. The intending Bidders have to apply in their letter head pad and must submit documentary evidence like VAT registration Certificate, Trade License, Certificate of manufacturer/ Manufacturer Authorisation Form (MAF)/ local agent of the mentioned solution in support of their past experience and specialization in the field. On being satisfied with documents submitted by the applicant, Tender document will be sold to the intending Bidders **from PCHAD, (ED), HO, IBBL, Yousuf Chamber (9th Floor), 20 Dilkusha C/A, Dhaka–1000** during office hours from **31.07.2018 to 29.08.2018** upon payment of Tk.3,000.00 (Three thousand) only in cash (non refundable). No Tender document will be issued/ received by mail. **A Pre bid Meeting** in this connection will be held on **13.08.2018 at 11.30 AM** at the Meeting Room of ED (9th Floor, Yousuf Chamber), 20 Dilkusha C/A, Dhaka.

02. Tenders will be received at the office of the undersigned up to **2:00 P.M.** On **30.08.2018** and will be opened at **2.10 P.M**. on the **same day i.e. 30.08.2018** at same place in presence of the Bidders who may like to attend the Tender opening.

03. An equivalent amount @ 2.5% (Two point five percent) of the total Tender value must be submitted along with the financial offer of Tender (attached with financial offer) as earnest money in favor of Islami Bank Bangladesh Limited in the form of Bank Draft/ Pay Order from any scheduled Bank of Bangladesh preferably from Islami Bank Bangladesh Limited without which the Tender shall be rejected outright.

04. Islami Bank Bangladesh Ltd. reserves the right to accept any Tenders and reject any or all Tenders without assigning any reason whatsoever. Islami Bank Bangladesh Limited is not bound to purchase the item(s) from the lowest bidder.

Senior Vice President