Bidding Document

VULNERABILITY MANAGEMENT SOLUTION

Last Date for Submission: **28th September, 2018 at 03:30 P.M.**
Tender Opening Date: **28th September, 2018 at 04:00 P.M.**

---

1. Background and Objective

The Bank of Khyber – ICT Security Department strives to improve information security posture on continuous basis, by identifying and addressing known weakness associated with information processing facilities. The main objective is to enhance vulnerability management program by systematically implementing a suitable enterprise vulnerability management solution to accomplish its mission in establishing a secure BOK IT environment and meet regulatory compliance respectively.

2. Scope of Work

2.1 Asset Compatibility:

- Solution should be able to scan all types of network devices like routers, firewalls, switches, load balancers without any dependency on any particular vendor
- Solution should be able to scan all types of Operating systems like Microsoft Windows (server and client end), flavors of Unix and Linux OS like HP-UX, Oracle Linux, Red Hat Linux etc.
- Solution should be able to scan multiple types of enterprise databases like Oracle DB, Microsoft SQL, MySQL etc.
- Solution should be able to scan virtual platforms like HyperV and VMWare ESXi etc.
- Solution should be able to scan Web Applications

2.2 Asset Scanning & Management

- Solution must support scanning of at least 512 IP addresses with scalability up to 5000 IP addresses
- Solution must perform discovery, vulnerability scanning and configuration assessment in a single scan.
- Solution must label unsafe checks and allow users to disable these on a per-scan basis.
- Solution should have the functionality to granular controls for managing scan speed and resource usage such as:
  - Maximum retries
  - Timeout Interval
  - Scan Delay
  - Packet-Per-Second Rate
  - Parallelism
- Solution should support the automatic discovery of virtual assets on:
  - Vmware vCenter
  - Vmware ESX/ESXi
  - Support hypervisor scanning of virtual assets on Vmware NSX
- Solution should be able to track devices that have been virtualized and may have common MAC and/or Hostnames.
- Solution should 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.
- Solution's scans should be user controllable, i.e. able to be started, stopped, paused and resumed at any time per user requirements.
- Solution should be able to schedule scans at specific starting dates and time, frequencies and maximum scan durations.
- Solution should be able to automatically pause scheduled scans if unable to complete within the predefined durations.
- Solution's unfinished scheduled scans should be able to automatically continue the scan where it previously stopped on the next scheduled session.
- Solution must be able to support both credentialed and non-credentialed scans which include but is not limited to:
  - File Transfer Protocol (FTP)
  - Microsoft Windows/Samba (v1 and v2) (SMB/CIFS)
  - Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)
  - Oracle
  - Simple Network Management Protocol (SNMP)
  - Secure Shell (SSH)

- Secure Shell (SSH) Public Key
- Telnet

- Solution must be able to support credentials login to database including but not limited to :
  - Microsoft SQL
  - MySQL Server
  - Oracle
- Solution should be able to provide a holistic view of the environment where users can drill down at any stage to explore, including but not limited to:
  - Assets
  - Vulnerabilities
  - Exploits
  - Malwares
  - Policies
  - Installed Software
  - Services
  - Users & Groups
  - Databases
  - Files & Directories Listing
- Solution should have the functionality to build a single database of discovered assets and detected vulnerabilities without relying on any third party tools.
  - Independently of scanning frequency
  - Independently of scanning type
- Solution should be able to support both IPv4 and IPv6 in the same installation.
- Solution should 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, software name and vulnerability type.
- Solution should support alert types out of the box like following :
  - SMTP
  - SNMP
  - Syslog
- Solution must be able to exclude vulnerabilities and assets from scans and reports.

2.3 Web Application Scan

- Solution should include built-in web application scanning capabilities against web technologies including but not limited to AJAX, ASP.NET 2.0 and Flash-based sites.
- Solution should support scanning of OWASP Top Ten vulnerabilities.
- Solution should support credential login through HTTP Form and Basic Digest authentication for scanning.
- Solution should support web spidering/crawling to gather security related information such as directory structures, files and applications running on the web servers.
- Solution should have the functionality to set scan rate such as thread per web server to control bandwidth consumption and scanning time.
- Solution should have the functionality to set limit of maximum directory level, maximum crawling time, maximum pages and maximum link depth.

2.4 Vulnerability & Risk Management

- Solution should have a vulnerability database that is updated on a regular basis automatically
- Solution should perform vulnerability checks across network, operating systems, web applications, Virtual environments and databases.
- Solution should support automatic scanning for specific vulnerabilities and browse the vulnerability database by category and type.
- Solution should have criticality rating to calculate aggregated risk scores of vulnerabilities in addition to asset criticality scores.
- Solution must provide both Quantitative Metrics as well as Qualitative (i.e. Critical, High, Med, Low) Metrics.
- Solution's risk score should include but not limit to vulnerability impact, likelihood of compromise, date of disclosure, exploit exposure and malware exposure.

- Solution must calculate risk score individually for each detected vulnerability which takes into consideration CVSS scoring, asset exploitability and susceptibility to available malware kits and exploit modules.
- Solution should have the functionality to set asset or group importance level to allow user to scale up or down the risk.
- Solution must have prioritization capabilities with respect to vulnerabilities and remediation tasks. Supplier has to describe how this is achieved in the solution during acceptance testing.
- Solution must have ability to display suggested vulnerability remediation solution or reference links for each discovered vulnerability within the web interface without online/internet access (with exception to respective knowledge base for each affected product/OS/application/devices vendor).
- Solution must be able to identify known exploits and malware kits associated with detected vulnerabilities.
- Solution should provide correlated list of:
  - Metasploit exploit modules available for each vulnerability
  - Malware kits available for each vulnerability

2.5 Policy Audit

- Solution should include built-in compliance checks such as PCI-DSS, CIS, NIST etc.
- Solution must centrally manage and modify policies and easily detect misconfigurations in scan environments

2.6 Report & Data Export

- Solution should provide built-in reports including but not limited to audit, baseline comparison, executive summary, PCI, policy compliance, policy details, remediation plan, top remediation, top policy remediation and vulnerability exception report.
- Solution should support base-line comparison reports
- Solution should support report template customization from default available ones.
- Customized reports should allow creation of new templates and inclusion of customized logo and title.
- Solution should be able to generate report based on scan groups, asset group (static or dynamic), tags (default and customized) and individual asset(s).
- Solution should support report scheduling capabilities. Application should be able to automatically send reports when scans are completed.
- Solution should be able to export reports in various formats such as but not limited to CSV, PDF and XML.
- Solution should include access controls to reports based on user roles.

2.7 Server Management

- Solution should include web-based management user interface through encrypted channels.
- Solution should support role based customization on a per user basis to allow granular controls and/or extend/restrict user permissions.
- Solution must support integration with Active Directory, Kerberos, or any LDAP compliant directory.
- Solution must include built-in diagnostic tools to display system status. Diagnostic tools shall be able to upload log files through encrypted channels for analysis.
- Solution should be able to perform backup and restore of database, configuration files, reports and scan logs.
- Solution must be able to perform both automatic & manual (i.e. online & separate offline) updates. Updating interval must be customizable within the solution.

2.8 Installation, Deployment and Integration

- Solution should provide distributed client/server architecture with unlimited scalability which includes a centralized management security console that is able to manage multiple scan engines for consolidated reporting and data aggregation.
- Solution must be able to operate on premise deployment, even without Internet access. Describe the solution's architecture. Detail all components and modules required to deliver the complete solution.

- Solution must provide agentless scanning support
- Solution must support deployment in both modes (i.e. virtual appliance or software-based) as required.
- Solution should not have any limit in terms of CPU & memory for each deployed scanner to provide higher performance or handle scans that are more concurrent.
- Solution must be able to scale beyond its initial deployment.
- Solution must be able to offer an API capability.
- Solution must support integration with major SIEMs and Incident Management solutions such as Logrhythm, QRadar, and Service Now etc.

2.9 IT Infrastructure Environment details

The IT infrastructure environment covers the below mentioned details:

SNo	Environment	Description
01	Operating System	Linux, Unix, Microsoft Windows (Server & Workstation flavors), CISCO IOS, Juniper and Fortinet etc.
02	System/Device Type	Servers, Work Stations/Desktop, Network Switches/Routers, Firewall, Wireless LAN, VOIP Telephony, biometric device etc.
03	Web Services / Applications	Web services, Apache, IIS, .Net Framework, Microsoft - business software & office products, Oracle Applications, Microsoft Exchange, etc.
04.	Databases	Oracle, MS SQL and MySQL

3. Technical Proposal Response Format

Bidder is required to submit its Proposal in accordance with the following Mandatory Requirements; failing to which the proposal will not be considered (as Technical Evaluation is based upon Mandatory requirements).

3.1 Mandatory Requirements

i. The bidder be registered with FBR and should provide its registration **NTN** certificate and Registration of Incorporation under the laws of Pakistan.

ii. The bidder should provide the Authorized Licensing Solution Partner **(LSP)** certificate.

iii. Bidder must provide at least **02** Purchase Order/Agreement/Completion Certificate for provision/deployment of the similar software with relevant reference / contact information for any Organization / Financial Institutions / Banking sector

iv. Bidder must provide **Undertaking on stamp paper** that it is not being blacklisted by any of the Provincial / Federal Government or organizations of the State / Federal Government in Pakistan. And must provide List of arbitration/legal suits/unsettled disputes with clients (if any) in last five years

v. The bidder must submit **Annual Audited Report** for the last 03 financial years. Annual Audit Report including Balance Sheet, Income Statement and Profit & Loss accounts along with auditors' notes for the last three (3) audited years should be submitted

vi. The bidder must have legal presence in Pakistan and must provide lists of its offices.

vii. The bidder should have enough Technical Strength at its end to complete the project within stipulated time. List of Staff (HR) of the Company along-with their profiles to be submitted

3.2 Technical Evaluation Criteria

SNo	Clause	Marks
A	**Company Portfolio**	
1	Number of Years the firm has been established (1 Mark for each year upto Max 10)	10
2	Number of Similar nature projects/deployments (1 Mark for each Project upto Max 10)	10
3	Number of Similar nature project/deployments in any Financial Institution (2 Mark for each Project upto Max 6)	6
4	Number of Offices across Pakistan (1 Mark for each Office upto Max 3)	3
B	**Financial Capabilities**	
1	Average Annual Turn Over of the bidder for the last 3 Years (upto 10 Million=2 Marks, upto 20 Million=4 Marks, upto 30 Million or above =6 Marks)	6
2	Audit Report for last 03 Financial Years	1
C	**Relevant Staff Assigned to the Project**	
1	Number of Certified Information Security Technical Resources (1 Mark for each Resource upto Max 2)	2
D	**Software Technical Assessment**	
1	**Vulnerability Assessment**	
1.1	Asset Discovery	3
1.2	Database Vulnerability Detection (DB2, MySQL, Oracle, etc.)	3
1.3	Malware Detection	3
1.4	Rule-based Remediation Prioritization	3
1.5	Support for Virtualized Assets	3
1.6	Asset Profiling (e.g.: IP, OS, Ports etc.)	3
1.7	Risk Analysis	3
1.8	Application Security Testing (e.g.: OWASP Top 10, CWE 25)	3
2	**Deployment Options**	
2.1	Software	2
3	**Flexibility and integration**	
3.1	Role-based access	2
3.2	Centralized dashboards	2
3.3	Integration with SIEM,GRC,NMS etc.	2
3.4	Integration with enterprise asset management tools	2
4	**Compliance and Reporting**	
4.1	Supports COBIT, PCI, HIPAA standards	2
4.2	Configuration benchmarking (CIS, SCAP, OVAL standards)	2
4.3	Asset/functionality based reports	2
4.4	Allows Customized reports	2
5	**Presentation of Proposed Solution**	**20**
Total Marks		**100**
Technical Qualification Marks are 60% of the Total Marks		**60**

Financial bids of firms who score at least 60% of the total marks on the technical evaluation will be opened before the representatives who wish to attend the financial bid opening.

Ratings for tender evaluation will be as follows:

Sr. No.	Description	Evaluation Weight-age
1.	Technical Proposal	70%
2.	Financial Proposal	30%

70 % weight-age will be given to Technical proposals of bidders while 30 % weight-age will be given to financial proposals. The formula for financial scoring is that the lowest bidder gets 30 points and the other bidders score 30 multiplied by the ratio of the lowest bid divided by the quoted price.

3.3 Training Capabilities

Bidder should indicate its training capabilities to provide training on proposed solution. It should also provide a detailed training schedule. Training premises (on–site) Interactive sessions and necessary equipment will be arranged by the bidder. Preference will be given to the bidder with certified trainers.

3.4 Warranty Period

The bidder shall give comprehensive (6) six months warranty after complete deployment under company strategy, certifying that the software confirm exactly to the specifications laid down in the contract. An amount equivalent to 10% of total payment (inclusive of 2% earnest money) shall be retained by BoK as performance warranty/defect liability for a period of 6 months of the actual date of complete sign off and Go Live of the software. In case of delay penalty may be imposed as per contract.

4. Financial Proposal Response

Bidder must submit its financial proposal in accordance with the following format: -

SNo	Description	Amount in PKR	GST	Total Amount in PKR
1	**Vulnerability Management Solution**			

4.1 Currency

All currency in the proposal shall be quoted in Pakistan Rupees (PKR).

4.2 Withholding Tax, Sales Tax and other Taxes

Bidder is hereby informed that the Bank shall deduct tax at the rate prescribed under the tax laws of Pakistan, from all payments rendered by any bidder who signs a contract with the Bank. Bidder will be responsible for all taxes on transactions and/or income, which may be levied by government.

4.3 Governing Law

This bidding document and any contract executed pursuant to this document shall be governed by and construed in accordance with the laws of Pakistan. The Government of Pakistan and all bidders responding to this bidding document and parties to any contract executed pursuant to this document shall submit to the exclusive jurisdiction to Courts.

Terms and Conditions

a) The Procurement Shall be conducted in accordance with the Khyber Pakhtunkhwa Procurement Rules 2014 on **Single Stage Two Envelope Procedure.**

b) The Bank of Khyber Invites two separate sealed envelopes, one for Technical Proposal and One for Financial proposal from Service Provider having legal presence in Pakistan for the provision and deployment, training and support of the required Vulnerability Management Solution.

c) Bidder is required to submit both sealed proposals to the office of the Head Procurement Division, The Bank of Khyber on or before **Friday 28th September, 2018 at 3:30Pm**. Tender Opening date is Friday **28th September, 2018 and Time is 4:00Pm** at The Bank of Khyber, Head Office.

d) Company should sign and Stamp BOK RFP and must attached with their Technical proposal.

e) Company seal / stamp must be fixed on both Technical Proposal and Financial Proposal.

f) All the firms applied for the Tender must provide documents in line with the Mandatory requirements and should qualify the Technical Evaluation Criteria. **If any firm fails to qualify the Technical Evaluation Criteria, then Financial Proposal of the same will not be opened.**

g) Any bid submitted Late and after due date and time or bid not complying with all required clauses in this bidding document are liable to be rejected.

h) Bid Security of two percent (2%) of the total bid amount in favor of the Bank should be attached with financial proposal in separate sealed envelope and should be submitted to Head Procurement Division, The Bank of Khyber.

i) All prices quoted must be inclusive of all Taxes applicable, such as GST, Income Tax, etc.

j) The prices quoted shall remain valid for 120 days, after the date of opening the tender.

k) Delivery of all items must be made within (3 – 4) weeks of issuance of purchase order.

l) In case of failure to provide the required deliverables under the specified time, Bid Security amount will be forfeited.

m) In case of consortium, the bidder must submit:

- The details of the consortium with roles and responsibilities of each partner.
- The original stamped consortium agreement shall be attached along-with the Bid Document.
- The same should be endorsed by an authorized representative of the prime bidder. The Prime bidder will be the single point of contact with the Bank for the project undertaking.
- No change in the constitution of the consortium (prime bidder/members of consortium / stakes of any member etc.) will be allowed without explicit approval of the Client.

n) The Bank of Khyber will not be responsible for any costs or expenses incurred by bidders in connection with the preparation or delivery of bids.

o) No negotiations and revised bids will be allowed.

Head Procurement, General Administration Department **24, The Mall, Peshawar, Head Office, The Bank of Khyber**
Phone: 091-5279690, 5274399
UAN: 091-111-95-95-95, Fax: 091-5286769