Prime Bank Limited
a bank with a difference

Prime/HO/FMD/2016/VA/

Facility Management Division

.....
.....
.....
.....

May 10, 2016

Sub: Request for submission of price proposal of Vulnerability Assessment Tool for Prime Bank Ltd.

Dear Sir,

Please know that Prime Bank Limited intends to purchase Vulnerability Assessment Tool for Prime Bank Ltd. For this purpose, we are inviting you to submit financial offer along with technical specification in your letterhead pad using following format:

Lot- A: Vulnerability Assessment Tool.

Solution Name	Model	Qty	Total Price in BDT (inclusive VAT & Tax)	Remarks

Terms & Conditions:

1. Delivery & Installation:
   A. As and when required up to price validity.
   B. The supplier will deliver & install the products to the Bank's selected location (anywhere in the country). No additional cost will be paid by the bank for transportation.
   C. In case of supply of inferior quality/defective goods; any change request by Prime Bank must be entertained.

2. Payment: Payment will be made within 30 (Thirty) days from receipt of bill from the Supplier. Payment will be made as per the following terms and conditions:
   A. Payment will be made after satisfactory installation of the equipment & subsequent certification of Information Security Division/ Concerned users.
   B. Bank will deduct VAT & AIT as per govt. rules.

3. Warranty: The bidder will cover system components, maintenance, support and updates of the software up to service period.

4. Support Level: The Supplier shall provide immediate response either by phone, e-mail, and fax or by person to any of the Purchaser's queries related to support and service.

5. Validity of the Rate: The quotation rate and other terms and conditions should cover a period of 06(Six) months from the date of submission of RFQ.

6. Paper & Documents: The supplier should have submitted the following paper & documents:
   A. Valid Registration/ownership document, VAT & TIN certificate, up-to-date Trade License, and up-to-date Bank Solvency Certificate.
   B. Distributorship or Sole Distributorship certificate.
   C. Copies of work-order(s) and performance certificate(s) of execution of same work with different commercial Bank/MNC

7. Technical specification: Technical specification is attached in page-2 and onward. Bidder's response will be filled up by participant companies.

Prime Bank Limited
a bank with a difference

Vulnerability Assessment (VA)

A vulnerability assessment surveys a network and identifies potential vulnerabilities that exist. However, it does not address the implications of a successful intrusion. A vulnerability assessment only lists what the potential vulnerabilities are, and does not investigate deeper to reveal the true threat to assets when vulnerability is exploited.

A vulnerability assessment generally includes below activities:

- Scans for potential vulnerabilities on a network
- Generate a list of Vulnerabilities
- Categorized vulnerabilities based on theoretical information
- Produce false positive
- Does not address connection between network connection

A. Required Technical specification of Vulnerability Assessment Tool

S/N	Feature	Detail
Architecture		
1	General Requirements	The VA solution should have following capabilities: • Can immediately reach to the perimeter systems. • Can be used directly from the browser. • Scale easily to handle new devices, users and locations. • Enable results to be stored in an objective, tamper resistant way for audits.
2	Both monitoring and scanning capabilities	The VA product should have both vulnerability scanning and an ongoing view of the systems and network security including making predictions about emerging "Zero Day" vulnerabilities or "Patch Tuesday" issues without requiring new scans.
3	Area of scan	The VA solution should be used to check systems everywhere - • On the Internet, • Inside PBL private network, • Endpoint systems • Passwords and identities • Mobile devices • Wireless networks • Web applications and services • Network systems and devices, and • The Cloud. A single tool, but need to have the consolidated view of our security.

S/N	Feature	Detail
4	Locations to handle	When the VA software will use internal PBL network to reach each of the devices being scanned, this would not create bottlenecks. The VA services should scan external, Internet-facing devices. The VA solution should to check systems in many locations at once. The solution should use secure, remotely-managed scanner appliances (either physical boxes or virtual machines) that can be placed in different portions of the network to make internal scanning efficient and minimize the impact on other infrastructure.
5	Open holes in existing firewall	It should not compromise the security by opening special ports in PBL firewall.
6	Integrating VA with other systems	The VA solution should have robust APIs for integrating with other security incident and event management (SIEM), risk management (ERM), or governance (GRC) solutions.
7	PCI DSS enlisted Approved Scanning Vendor	The VA solution should be enlisted (ASV) with PCI DSS, as such VA Solution should fulfill compliance of PCI DSS scanning requirements.
8	Minimum Required Coverage	The Solution should cover up to 128 Internal IP's and 5 External IP's. Both Internal and External IP should be changeable.
Scanning		
9	Reaching the VA to all of the systems	The VA solution must be able to scan all the systems, even as they move in and out of the network. The solution should handle Cloud, perimeter and internal devices together in a consistent way. It should discover devices that are lost or hiding in the network.
10	The VA should discover what's actually in the network	The VA solution should search through the perimeter, internal networks, and cloud environments to discover and catalog the devices actually running there.
11	Dynamic organization of devices	The VA solution should discover and arrange all devices into groups for scanning and reporting. The VA systems should do this dynamically based on what's found on the devices –the OS, its networking, software, IT assets, the applications and services running on them, including IPv6, virtual and cloud-hosted assets, etc. It should have techniques like "tagging" to programmatically apply labels to each device we encounter. It should integrate asset information with third-party asset inventories

S/N	Feature	Detail
		such as Active Directory (AD), LDAP and VMware, vCenter and organize and dynamically update assets into logical groups.
12	Scanning large numbers of devices efficiently	The VA solution should have scalability, allowing to scan portions of the network in parallel and automatically consolidate the results into a single report, which would accelerates scanning without overloading the network. It should scale seamlessly from a few devices to millions.
13	Scanning automatic or scheduled	The VA solution should be able to have scans run on any schedule (such as during maintenance windows) or even to repeat continuously.
14	Combining vulnerability data from industry-standard sources	The VA solution should combine vulnerability data from industry-standard sources such as CERT, software vendors such as Microsoft, and information received from world-wide networks of customers to look for solutions that rigorously test each vulnerability definition for accuracy. The Solution should compare, track and benchmark internal policies against industry best practices and benchmarks such as FDCC, CIS and USGCB and leverage policy frameworks such as SCAP.
15	Adding new vulnerability signatures	The VA system should be able to use new vulnerabilities as soon as they are published by the VA vendor.
16	VA authentication for deeper scanning	The VA solution should allow us to specify credentials for securely logging into devices, databases or applications.
17	Industry-standard scanning accuracy	The VA solution should use industry-standard processes such as Six Sigma for measuring accuracy.
18	Using the VA by multiple people simultaneously	The VA solution should allow different people to scan and report simultaneously without interfering with each other.
19	Protecting VA data	The VA solution should stores vulnerability data away from users to prevent tampering, and protect scan data against eavesdropping and tampering.
20	Automated Work Flow	• Exclude vulnerabilities from reports as needed based on corporate policies regarding acceptable use and risk from compensating controls. • Administer exceptions and policy overrides. • Establish expiration dates to ensure you are appropriately re-evaluating risk.

S/N	Feature	Detail
Reporting		
21	The VA tailor reports to different audiences	The VA solution should distill vast amount of data they collect into insights to drive prompt security actions. The solution should give us differing levels of information, from executive-level scorecards of the overall security to detailed drill-down reports.
22	Offering predictive analysis	The VA solution should keep track of the state of each device in order to predict which devices might be vulnerable to new "Zero-Day" attacks or "Patch Tuesday" issues without requiring new scans.
23	Highlighting changes across scans	To avoid revisiting old issues, the VA solutions should track whether each vulnerability found is: new, being worked on, already fixed, or accepted as not worth fixing. The solution should provide "differential reporting" that highlights changes from one scan to another.
24	Prioritizing the vulnerabilities in reports	The Vulnerabilities should be ranked by severity, based on industry standard, that could help us efficiently prioritize how and when to address each issue and is particularly important for complying with mandates which require proof that severe vulnerabilities are being promptly identified and fixed.
25	Patch-centric reporting	The solution should organize vulnerabilities according to the patches that address them.
26	Reports to show Compliance	The VA solution should conduct security assessments and run reports to certify compliance with regulations and native support for key mandates such as PCI, HIPAA, NERC, FISMA, SANS Top 20 as well as the ability to properly customize reports to our individual needs.
Fixing / Remediation		
27	Information about the underlying cause does the VA provide about each vulnerability	The VA solution should exist solution to eliminate vulnerabilities, not just find them. The VA solution should provide detailed descriptions of each vulnerability as well as links to the vendor updates or patches needed to fix it.
28	Providing automated trouble-ticketing	The VA solution should allow remediation tasks to be assigned according to users' specific roles and can track what gets fixed and when. The VA system should provide automated notification of tickets as well as comprehensive reporting on ticket status. The solution should also provide executive summaries across groups of devices of as well as detailed drill-downs per device, vulnerability and user.