Common Services Division
Corporate Head Office, Dhaka

March 12, 2026

Request for Quotation (RFQ): Sealed Quotation for Supply, Installation and Commissioning of Vulnerability Management (VM) solutions.

1.1 Scope of Bid

Shahjalal Islami Bank PLC. (Hereinafter referred to as "the Bank") wishes to receive bids from the bona fide firms for supply, installation and commissioning of Vulnerability Management Tools as mentioned above.

1.2 Bidder's qualification

a. Local bidder must be a registered company in Bangladesh having proven and substantial market presence in selling IT Security related software solutions for the last 2 years (preferable) in Financial/Telecom/Government sector in Bangladesh.
b. Local bidder of the Vulnerability Management solution supplier must be an OEM authorized direct reseller/partner for a minimum of last two (2) years (preferable) proving its strong affiliation as well as expertise of the solution being offered.
c. Bidders shall possess his own office and adequately trained and experienced manpower to install, configure and maintain the supplied products.
d. Bidders should submit the documentary evidence of Tax Identification Number (TIN), Business Identification Number (BIN) and Value Added Tax (VAT) as a proof of taxation obligations imposed inside and outside of Bangladesh including under the laws and regulations of the country of its origin.
e. Bidders should have the capacity to solve any support related issue occurred between the client and the mother company of the product.
f. The offered solution should capable enough to be installed minimum two different types of proprietary operating systems to qualify the eligibility of the offered product.
g. 24x7 support need to be ensured.

1.3 Documents comprising the bid

a. Technical Description of the deliverables to demonstrate the specified technical requirement.
b. Schedule for financial proposal.
c. Valid Trade License and Company Profile along with Memorandum of Association and Article of Association.
d. E-TIN and VAT Certificate.
e. Name, contact number and e-mail address of the Contact person(s).
f. Proof of Experience.
g. List of corporate clients in Bangladesh for such solution.
h. Proof Certificates as Authorized Reseller/Authorized Dealer/Supplier from the manufacturer to be submitted.
i. All Proper documents, brochure, data sheet, technical spec papers of mentioned Products have to be provided by the bidder in the Technical Proposal.
j. Number of security experts of offered solution with names and contacts. Preferable to provide relevant certifications as proof.
k. To fulfill the bidder's qualification all required documents should be provided as a proof of evidence.
l. All required documents needs to be provided as a proof of evidence to fulfill the need of supplier qualification.

1.4 Bid prices

Bidders shall quote the price excluding VAT in US Dollars (USD) (The payment of the products will be made in BDT at the "Bank's USD BC selling rate" at the date of delivery of the solution). Related VAT to be borne by the bank. Required product will be 03(three) years license which includes all costs.

1.5 Bid validity

Bid shall remain valid for a period of **150 days** from the date of opening of technical 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 thereto shall be made in writing. A bidder agreeing to the request will not be permitted to modify its bid.

1.6 Sealing and marking of bid

The envelope shall:

a. Be addressed to the Bank at the following address: **Member Secretary, Procurement Committee, Shahjalal Islami Bank PLC.,Corporate Head Office, Common Services Division (2nd Floor), Shahjalal Islami Bank Tower, Plot-04, Block- CWN(C), Gulshan Avenue, Gulshan, Dhaka-1212.**
b. Bidder(s) should submit the financial and technical offer in separate envelope mentioning the name of the offer and both envelopes must be submitted together in a single envelope.
c. In addition to the above requirements, the envelope shall indicate the name and address of the bidder to enable the bid to be returned unopened in case may be declared "late" pursuant to clause 1.9.
d. If the envelope is not sealed and marked as above, the Bank will assume no responsibility for the misplacement or premature opening of the bid.

1.7 Bid Security / Earnest Money

The bidder shall submit 2 % (Two) of their bid price in the form of Payment Order/ Bank Guarantee as bid security in favor of Shahjalal Islami Bank PLC. The Bid Security/ Earnest Money should be enclosed on the top of the technical offer. 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 150 days from the date of bid opening. Selected bidder will get back the Bid Security/ earnest money on submission of performance security.
The bid security may be forfeited if
(a) The bidder withdraws its bid during the period of bid validity.
(b) A successful bidder fails to sign the contract.
(c) A successful bidder fails to furnish the performance security

1.8 Deadline of bid

The bidder must submit the bids in original (sealed), duly marking the envelope as addressed at the following no later than **1:00 p.m. on April 05, 2026.**

1.9 Late Bids

Any bid received by the Bank after the deadline for submission of bid prescribed in clause 1.8 may be rejected and returned unopened to the bidder.

1.10 Evaluation of proposals

The Bank will choose the offer that will be more comprehensive and that conform the relevant required product. Information relating to the examination, clarification, evaluation and comparison of bids and recommendations for the award of a contract shall not be disclosed to bidders or any persons not officially concerned with such process until the award to the successful bidder has been announced.

1.11 Price Negotiation

The Bank may request competent bidders to negotiate the price or any other relevant queries. Representative of the Bidders must have authorization for price negotiation. Bank will choose the successful bidder, after price negotiation, considering other performance and quality of products which are deemed fit by the Bank.

1.12 Award of Contract

Subject to Clause 1.10 &1.11, the Bank will award the Contract to the successful bidder.

1.13 Bank's right to accept any bid and to reject any or all bids

Notwithstanding Clause 1.12, the Bank reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the grounds for the Bank's action.

1.14 Notification of Award/Work Order

Prior to expiration of the period of bid validity prescribed by the Bank and after successful negotiations (if any), the Bank will notify/issue work order in favor of the successful bidder that his bid has been accepted. The notification of award/work order may constitute the updated terms and conditions and basic formation of the Contract.

1.15 Performance Security

The successful vendor will have to deposit an amount equivalent to 5% (five) of the total work order/contract value as performance security in the form of Payment Order / Bank Guarantee in favor of Shahjalal Islami Bank PLC. while accepting the Work Order. Mentioned performance security would be returned after 03(three) years from the date of issuance of the Work Order.

1.16 Product Delivery

15 (fifteen) calendar days from the date of receiving the Work Order.

1.17 Warranty

Warranty of the product shall be considered on the date from which the license will be activated in OEM Website or by other means of relevant justification. The vendor should make the overall system ready and hand over the same to the officials within 15 working days from the date of license activation.

1.18 Security Money

An amount equivalent to 5% of total work order/product value will be considered as security money. Security money amount will be deducted from the bill and retained up to three (03) years from the date of live operation of the product. Security money will be returned after above mentioned stipulated time period of three (03) years. Security money may be forfeited in case of violation of support or any other issues mentioned in RFP.

1.19 Penalty

In case of failure or any kind of delay regarding delivery of the product within due time mentioned in clause 1.16 or the violation of the clause 1.17, vendor will be liable to pay 1% of the total work order value, as penalty, to the bank for delaying each week after the due date. Upon reaching the penalty to 3% of total Work Order/Contract value, the performance security as well as the Work Order may be forfeited on sending a letter to the vendor.

However, Bank must be informed for any foreseeable delay due to uncontrolled situation prior to exceed the delivery deadline mentioned in clause 1.16 or product handover mentioned in clause 1.17 which may be considered by the bank if situation justify such delay and the decision of procurement committee of the bank will be final.

1.20 Payment

Full Payment will be made after successful **supply, installation, testing and commissioning** of the product as well as confirmation from OEM (through site/e-mails) to fulfill the requirements of RFQ (like License quantity, License support duration etc.) after deducting security money.

1.21 Withholding Sales Tax

The bidder is hereby informed that the Government shall deduct tax at the rate prescribed under the Tax Laws of Bangladesh, from all payments for services rendered by any bidder who signs a contract with the Bank. The bidder will be responsible for all taxes on transactions and/or income, which may be levied by the bank. If bidder is exempted from any specific taxes, then it is requested to provide the relevant documents with the proposal.

1.22 Contact Person

The bidder may contract with below mentioned official(s) for any queries.

For Technical queries:	For Financial queries:
Zabedul Hoque Chowdhury ICT Security Department e-mail: zabedul4463@sjiblbd.com Cell: + 88011814874480	S. M. Tarequl Islam Hyder Common Services Division e-mail: tarequl4471@sjiblbd.com Cell: +8801755556361, +8801712480201

Zahid Hasan 12/03/26
SVP & Head of ICT Security Department

Abul Bashar Md. Zafry
EVP & Head of CSD

شاه جلال اسلامي بنك بي إل سي

Shahjalal Islami Bank PLC.
Committed to Cordial Service

শাহজালাল ইসলামী ব্যাংক পিএলসি.
আন্তরিক সেবায় প্রতিশ্রুতিবদ্ধ

Common Services Division
Corporate Head Office, Dhaka

Financial Offer
of
Vulnerability Management(VM) Solution

Common Services Division, Corporate Head Office (CHO)
Plot # 04, Block # CWN (C), Gulshan Avenue
Gulshan, Dhaka-1212.

Common Services Division
Corporate Head Office, Dhaka

Format of the Financial Offer

Option:01

S/L	Product Description	Price (USD) excluding VAT & including Tax
1.	Vulnerability Management (VM) Solution (Required product will be 03 (three) years licence including all support & service costs)	USD……../-
	Total	USD……./-

- All prices are including Tax & excluding VAT (VAT to be borne by the bank).
- All Prices are to be quoted in USD.
- The payment of the products will be made in BDT at the "Bank's USD BC selling rate" at the date of delivery of the product.

Option:02

S/L	Product Description	Price (USD) excluding VAT & including Tax
1.	Vulnerability Management (VM) Solution (Required product will be 03 (three) years licence including all support & service costs)	USD……../-
2.	Additional features: Specification of Attack Surface Management(ASM) for 25 IPs	USD……../-
	Total	USD……./-

- All prices are including Tax & excluding VAT (VAT to be borne by the bank).
- All Prices are to be quoted in USD.
- The payment of the products will be made in BDT at the "Bank's USD BC selling rate" at the date of delivery of the product.

*****Vendors may provide pricing for both options or for Option:01. Bank will procure either Option:01 or Option:02**

شاه جلال اسلامي بنك بي إل سي

Shahjalal Islami Bank PLC. শাহ্‌জালাল ইসলামী ব্যাংক পিএলসি.

Technical Specification
Of
Vulnerability Management Solution

ICT Security Department, Corporate Head Office (CHO)
Plot # 04, Block # CWN (C), Gulshan Avenue
Gulshan, Dhaka-1212.

Technical Specification of Data Vulnerability Management (VA) Solution

Table-A: Full form of acronyms used in this RFP

S/N	*Acronym*	*Full Form*
1.	ACL	Access Control List
2.	CIS	Center for Internet Security
3.	AES	Advance Encryption Standard
4.	DB	Database
5.	DDOS	Distributed Denial-of-Service (DDoS)
6.	DC	Data Center
7.	DMZ	Demilitarized Zone

8.	DR	Disaster Recovery
9.	FIPS	Federal Information Processing Standards
10.	HTTP	Hypertext Transfer Protocol (HTTP)
11.	HTTPS	Hypertext Transfer Protocol Secure
12.	IIS	Internet Information Services (IIS)
13.	IP	Internet Protocol
14.	LDAP	Lightweight Directory Access Protocol
15.	MAC	Media Access Control
16.	MFA	Multifactor Authentication
17.	MSTSC	Microsoft Terminal Services Client MSTSC *Illustration:* Command for Remote Desktop Services
18.	OEM	Original Equipment Manufacturer
19.	OpenSSH	The open-source version of the Secure Shell (SSH)
20.	OS	Operating System
21.	OTP	One Time Password
22.	PAM	Privileged Access Management
23.	PCI DSS	Payment Card Industry Data Security Standard
24.	PuTTY	Popular SSH and Telnet Client
25.	RADIUS	Remote Authentication Dial-In User Service
26.	RDP	Remote Desktop Protocol
27.	RFP	Request for Proposal
28.	SAML	Security Assertion Markup Language
29.	SIEM	Security Information and Event Management
30.	SNMP	Simple Network Management Protocol
31.	SSH	Secure Shell
32.	SSO	Single Sign-On
33.	SWIFT CSP	SWIFT Customer Security Programme
34.	TACAS	Terminal Access Controller Access-Control System
35.	TIN	Tax Identification Number
36.	TSE	Terminal Server Edition
37.	TTY	TeleTYpe
38.	VPN	Virtual Private Network
39.	VAT	Value Added Tax
40.	WinSCP	Windows Secure Copy.

Bidders are to complete the response to the tables presented in this section. The responses should be provided with necessary evidence / explanation.

SCOPE:

a) Capable to handle unlimited devices.
b) License Type: **512 IP and 05 (Five) Web application.**
c) Solution must provide industry standard features.
d) Bidder shall provide end to end solution including all VA applications required to meet requirement mentioned in this RFP. Performance should be seamless.
e) 25 IP for Attack Surface Management (as additional feature)

2HC

Table-B1 (to be filled in by Bidder)

Item	*Question / Requirement*	*Bidder Response*
1.	Year of Establishment	
2.	VAT / TIN / Tax	
3.	No of Employees	
4.	Number of security professionals with certificate	
5.	No of Banking Clients for security solution in Bangladesh (with completion certificate).	
6.	No of Non-Banking Clients for security solution in Bangladesh (with completion certificate).	
7.	No of Banking clients for security solution considering global aspect.	
8.	Name of the operating systems where the bank can install the offered product (software / connectors / others) at inhouse environment.	
9.	What would be the minimum and recommended infrastructure (hardware, operating system, software and database) requirements to operate the solution in DC.	
10.	Comply with RFP.	

Compliance Status	**No of issue**
Complied	
Partially Complied	
Not Complied	

Table-B2 (to be filled in by Bidder)

Type	
OEM Name	
Product Name	
Product Version	
Solution Origin	
Licensing Mode	
Options for additional license (please describe)	

2.4.2

Technical Specification of the VA Solution

Note: Partial responses should be clarified properly

Table-C: Architecture

S/N	Requirements	Compliance (Yes/No/Partial)	Description
	Architecture		
1.	Describe your solution's architecture, including all components.		
2.	The solution must provide an integrated storage model that does not rely on a third-party database product.		
3.	The solution must include the option for agents that provide vulnerability assessment and security configuration assessment.		
4.	The solution must provide a comprehensive and fully-documented API for automation of processes and integration with 3rd party applications.		
5.	The solution must be able to monitor network traffic continuously to detect and assess short-lived systems and hard-to-scan devices, such as sensitive IoT systems.		
6.	Scanners must be managed by the platform, e.g. updates to vulnerability detections, code and other updates.		
7.	The solution must be able to use groups of scanners in a single job.		
8.	The solution must be able to scan assets on customers' internal networks as well as assets which are external facing / publicly accessible.		
	General		
9.	The solution must fully integrate vulnerability assessment (scanning) and security configuration assessment to include combined licensing and consolidation of data, analysis, and querying.		
10.	"The solution should support all the below Vulnerability Detection methods natively: - Active Network-based Scanning - Agent Based Scanning		
11.	The solution must offer predictive prioritization of remediation based on business risk.		

2nd C

12.	The solution's offering must include 24/7/365 global technical support.		
13.	The solution must include automatic updates of new vulnerability detections/checks.		
14.	The solution must be able to resolve multiple IPs to a single asset, for assets that have multiple IPs at one time or over time.		
15.	The solution must provide an elastic licensing model to ensure the product continues to function without interruption when the license limit is temporarily exceeded.		
16.	The solution should have ISO27001, PCI DSS and SWIFT CSP (preferable) compliance certifications.		
	Access Control		
17.	The solution must provide role-based access control (RBAC) to control user access to specific data sets and functionality.		
18.	The solution must provide the ability to accept or modify risk for vulnerabilities, with such functionality restricted by user role and any vulnerability risk acceptance documented.		
19.	The solution must have the ability to ensure that certain IPs or ports can be blocked from scanning.		
20.	The solution must support Single sign-on (SSO) authentication methods.		
21.	The solution must be able to define and manage user groups, including limiting scan functions and report access.		
	Scanning		
22.	The solution must provide an easy-to-use GUI for the user to create vulnerability scan using quick actions menu.		
23.	The solution must support a variety of scan engine platforms to include Windows, Linux, macOS, as well as virtual-based appliances.		
24.	The solution must support multiple distributed scanning engines managed by a central console.		
25.	The bidder mentions the list of operating systems that are supported by the offered solutions		
26.	The solution must provide the ability to deploy unlimited scanners at no additional cost.		
27.	The solution must include the ability to schedule scan blackout windows to prevent scanning during prohibited hours.		
28.	The solution must provide automatic licensing provisioning with no maintenance required.		

2.11.2

29.	The solution must provide the ability to configure ports, protocols, and services for connections to scanners deployed throughout the network.		
30.	The solution must be configurable to allow for scan throttling to prevent generation of traffic that could disrupt normal network infrastructure.		
31.	The solution must allow entry and secure storage of user credentials, including Windows local and domain accounts, as well as Unix/Linux credentials using su and sudo privileges over SSH for authenticated scanning.		
32.	The solution must provide the ability to escalate privileges on target systems from normal user access to root/administrative access.		
33.	The solution must support customized scan scheduling, including the ability to have scans run at designated times, with predetermined frequency.		
34.	It is preferable that the solution should able to perform sensitive data searches to discover sensitive data at rest on Windows, UNIX and Linux systems.		
35.	The solution must be able to offer centralized scan and scan policy management.		
36.	The solution must provide for an "auto-aging" license model to ensure stale or retired assets no longer count against the license.		
37.	The solution must provide single Console page for provide the user name, password, targeted IP address, compliance set, application, DB etc.		
38.	The solution must provide an easy-to-use GUI for the user to create vulnerability scan using quick actions menu.		
39.	The Solution shall provide complete, accurate, and scalable web security and enables banks to assess, track, and remediate web application vulnerabilities.		
40.	The Solution shall include web application scanning capabilities against all web technologies.		
41.	The Solution must provide automated crawling and testing of custom web applications to identify vulnerabilities including Cross-site scripting (XSS), CSRF and SQL injection.		
42.	The Solution shall be able to Detect, identify, assess, track and remediate OWASP Top 10 risks, WASC threats, CWE Weaknesses, and web application CVEs.		
43.	The Solution shall support credential login through HTTP Form and Basic Digest authentication for scanning.		
44.	The Solution shall support web spidering/crawling to gather security related information such as directory structures, files and applications running on the web servers.		

45.	The 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.		
46.	The Solution shall have the functionality to exclude scan by HTTP daemon and path.		
47.	It is preferable that the solution should be able to Identify and report malware present in websites and apps.		
48.	The Solution shall have large vulnerability database to check.		
49.	The Solution should provide Centralized management – to be able to apply policies consistently across application.		
50.	The 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.		
51.	The Solution should be able to Prioritize remediation and focus on the most critical flaws.		
52.	The Solution should suggest remediation actions for the identified weaknesses.		
53.	The Solution should allow to check status of the scan in real time.		
54.	The Solution should be able to perform incremental scans.		
55.	The Solutions should provide interactive dashboard lets one understands the security of web applications at a glance.		
56.	The Web Application Scanner should have following Capability: a) Automated web application scanning capability b) Internal web application scanning capability c) External web application scanning capability d) API's scanning capability e) One concurrent scanning with unlimited scanning capability		
	Asset Discovery		
57.	The product must support an asset discovery capability that does not count against licensing.		
58.	The solution must provide integrated web and database service discovery.		
59.	The solution must be capable of detecting services that are running on non-standard ports.		
60.	The solution must be capable of detecting services configured not to display connection banners.		
61.	The solution must be capable of testing multiple instances of the same service running on different ports.		
62.	The solution must be capable of scanning dead hosts (devices which do not respond to ping).		
63.	The solution must support the optional use of netstat for		

2.11.2

	rapid and accurate enumeration of open ports on a system when credentials are supplied.		
64.	The solution must support the use of SMB and WMI for scanning Windows systems.		
65.	The solution must be capable of automatically starting remote registry services on Windows systems when performing a credentialed scan, then automatically stopping the service again once the scan is complete.		
66.	The scanner must support secure shell (SSH) with the ability to escalate privileges for vulnerability scans and configuration audits on Unix systems.		
67.	The solution must provide the ability to tune scan policies for minimal impact on networks and targets.		
	Vulnerability Assessment		
68.	The product must provide both authenticated and non-authenticated network-based scanning of target systems.		
69.	The product must not rely on any 3rd party scanners for vulnerability scanning.		
70.	The solution must be capable of agentless and agent-based testing for both local (authenticated) and remote (non-authenticated) vulnerability detection without the need for a client-side agent installed on the target device.		
71.	The solution must be capable of agent testing for local vulnerability detection at no additional charge.		
72.	The solution must provide an externally-hosted scanning service for scanning perimeter networks.		
73.	The solution must be capable of tracking DHCP changes by associating scan results of a given system with something other than the IP address.		
74.	"The solution GUI must include pre-configured vendor provided scan templates such as the: - Host Discovery - Basic Network Scan - Credential Patch Audit - Policy Compliance Auditing - Audit Cloud Infrastructure"		
75.	" It is preferable that the solution GUI must include tactical scan templates on specific threats such as the: - Log4Shell - PrintNightmare - ProxyLogon: MS Exchange - Shadow Broker - Solarigate - Spectre and Meltdown - WannaCry - ZeroLogon - Badlock		

2-11-C

	- Bash Shellshock - DROWN - Intel AMT Security Bypass"		
76.	The solution must detect and rank issues, risks, and vulnerabilities. It must also provide detailed information regarding the nature of the risk and recommendations to mitigate it.		
77.	The solution must include detailed output of scan findings to include information such as DLL versions expected and found.		
78.	The solution must be CVE compatible and provide at least 10 years of CVE coverage.		
79.	The solution must provide patch auditing for Microsoft operating systems and applications to include Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008 / 2008 R2, Windows Server 2012 / 2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange, and more.		
80.	The solution must provide patch auditing for all major Unix operating systems to include macOS, Linux (multiple distributions), Solaris, IBM AIX, HP-UX, and more.		
81.	The solution must provide coverage for third-party applications vulnerability such as Java and Adobe.		
82.	The solution must provide integration with patch management systems for patch auditing and delta reporting against scan findings such as Microsoft WSUS/SCCM, Red Hat Satellite, IBM Tivoli Endpoint Manager (formerly BigFix), Symantec Altiris, an Ques/Dell KACE.		
83.	The product must provide predictive vulnerability prioritization that uses real-time threat intelligence and machine learning algorithms to score vulnerabilities and predict which ones are most likely to be exploited in the near future.		
84.	"The solution must provide vulnerability prioritization context that helps users understand the key factors influencing each vulnerability score as follows - Threat Recency - Threat Intensity - Exploit Code Maturity - Product Coverage - Threat Intelligence Sources"		
85.	The solution must include vulnerability scoring according to the Common Vulnerability Scoring System (CVSS) v3.1 or later.		
86.	The solution must provide vulnerability exploitability information from 3rd party sources such as Core Impact, Metasploit, and Canvas.		

2112

87.	The solution must provide information about existence of exploit kits for a given vulnerability, including a summary of vulnerabilities that are exploitable by malware and affected assets.		
88.	The solution must track dates for vulnerability discovery and observation that can be used in filtering and reporting in time based filters.		
89.	The solution must allow selected vulnerability and configuration tests to be enabled or disabled during scheduled scans.		
90.	The solution must not be dependent on operating system ability to schedule tasks.		
91.	The solution must accurately track assets and their vulnerabilities, including highly dynamic IT assets like mobile devices and virtual machines instances.		
92.	"The solution must support and include Microsoft Active Directory scan to detect commonly exploited weaknesses such as the: - Kerberoasting - Weak Kerberos encryption - Kerberos pre-authentication validation - Non-expiring account password - Unconstrained delegation - Null Sessions - Kerberos KRBTGT - Dangerous trust relationship - Primary Group ID integrity - Blank Passwords"		
	Security Configuration Auditing		
93.	The solution must be capable of agentless compliance auditing without the need for a client-side agent installed on the target device.		
94.	The solution must support agent-based security configuration assessment based on CIS, PCI and DISA-STIG benchmarks.		
95.	The solution must provide security and configuration auditing benchmarks for regulatory compliance standards and other industry and vendor best practice standards. The bidder must list the supported benchmarks (e.g., PCI DSS 3.x / 4.x, HIPAA, CIS Benchmarks, NIST, etc.).		
96.	The solution must provide security and configuration auditing benchmarks for vendor best practices such as Microsoft, Linux, MDM solutions such as VMware AirWatch, routers and switches, firewalls, etc.		
97.	The solution must provide security and configuration auditing benchmarks for vendor best practices such as Microsoft, Linux, MDM solutions such as VMware		

2.11.C

	AirWatch, routers and switches, firewalls, etc.		
98.	The solution must provide auditing of Microsoft operating systems for security and configuration settings. List the operating systems and versions supported with available benchmarks.		
99.	The solution must provide auditing of all major Linux/Unix operating systems for security and configuration settings. List the operating system vendors and versions supported with available benchmarks.		
100.	The solution must provide auditing of databases for security and configuration settings. List the database vendors and versions supported with available benchmarks.		
101.	The solution must provide auditing of applications for security and configuration settings. List the application vendors and versions supported with available benchmarks.		
102.	The solution must provide auditing of public cloud (e.g., AWS, Microsoft Azure, Salesforce) and cloud-native infrastructure (e.g., Docker, Kubernetes) for security and configuration settings. List the cloud infrastructure vendors and versions supported with available benchmarks.		
103.	The solution must provide auditing of personally identifiable information (PII) and other sensitive content. List the content auditing benchmarks available.		
104.	The solution must allow audit policies to be customizable for organizational specific needs.		
105.	The solution must provide CIS Certified Benchmarks.		
106.	The solution must offer SCAP support.		
107.	The solution must offer offline configuration auditing		
108.	The product must not rely on any 3rd party scanners for compliance auditing / security configuration assessment.		
109.	The Solution CIS controls should be selected and customized according to the Bank's security policies.		
110.	The solution should support the latest out-of-the-box CIS benchmark releases of operating systems, databases, applications and network devices.		
	Workflow		
111.	The solution must aggregate the results of individual scans into cumulative vulnerability views with filtering and analysis to allow drilldown and pivot capabilities.		
112.	The Solution should have intelligence to avoid overlapping scans on the same assets.		
113.	The solution must provide comprehensive filtering of aggregate vulnerability results with drilldown capabilities.		
114.	The solution GUI must support the custom creation of		

211.C

	frequently used filters to provide usage convenience of commonly used investigation functions.		
115.	The solution GUI must have the ability to create and add own business context to assets by tagging them with descriptive metadata.		
116.	The solution shall have capabilities to generate logging and audit-trails for actions performed by the users.		
	Reporting		
117.	The solution must provide the ability to automate reporting by being able to schedule reports.		
118.	The solution must provide the ability to produce ad hoc reports while viewing results in the console.		
119.	The solution must support the ability to produce reports in the following report formats: PDF, CSV, HTML, formats.		
120.	The reports must have the ability to include hostnames (NetBIOS, DNS) along with IP addresses.		
121.	"The solution must provide out-of-the-box reporting templates such as the: - Authentication Summary Report - Exploitable Vulnerabilities Report - Mitigation Summary Report - Outstanding Remediation Tracking Report - Prioritize Assets Report - Unsupported Software Report - Vulnerability Detail Report - Vulnerability by Common Ports"		
122.	The reporting feature must be able to create and customize reports with out-of-the-box Widgets and Chapters using a point and click GUI		
123.	The reporting feature must provide the ability to schedule a report execution to either run once at a future time or scheduled execution.		
124.	The Solution should have pro-active in Scanning Activity Management.		
	Dashboards		
125.	The solution must include customizable graphical and list based dashboard elements for displaying vulnerabilities and status of the assessed environment.		
126.	The solution dashboard must be configurable to support the creation of illustration charts (Ring/Bar) and Table.		
127.	The Solution shall be capable of performing network wide discovery and shall have capabilities to identify type of system/service (e.g., Applications, network topology, switches, firewall, databases, mail-server, desktops, etc.)		
128.	The Solution must have a customizable dashboard with vulnerability and threat data including but not limited to: Sites, Assets, Vulnerabilities, Exploits, Malwares, Policies-		

2.4.C

	Installed Software, Services, Users & Groups, Databases Files & Directories Listing.		
129.	The solution dashboard must provide must provide cyber exposure news feed that provide insights into most recent blog posts related to Cyber Exposure incidents.		
130.	The solution must have end-to-end workflows & real-time, interactive dashboards.		
	Data Security		
131.	The solution must support Single sign-on (SSO) authentication methods.		
132.	The solution provider must support the customer data stored within Asia Region.		
133.	How long is active (network) scan data retained?		
134.	If a customer discontinues service, how long is data retained? Can it be downloaded by the customer?		
135.	Describe your key management process.		
136.	Describe your privacy or security certifications.		
137.	Describe your back-up procedures. Is data replicated?		
138.			
	Additional Feature: - Specification of Attack Surface Management (ASM)		
139.	The bidder should provide a solution capable of discovering, inventorying, and maintaining a centralized, continuously updated asset repository covering devices, applications, users, cloud resources, and security controls across the entire environment.		
140.	The bidder should ensure the solution enriches asset data with contextual risk intelligence, including vulnerability status, threat intelligence, asset criticality, and operational context.		
141.	The bidder should provide impact mapping and dependency visualization capabilities, including asset relationship mapping and blast radius analysis to support incident impact assessment.		
142.	The bidder should provide capabilities to identify externally exposed assets, services, ports, and shadow IT to clearly define the organization's external attack surface.		
143.	The bidder should ensure centralized remediation management, including task assignment, tracking, workflow coordination, and SLA monitoring.		
144.	The bidder should provide machine learning–powered detection of missing security controls, including identification of assets without endpoint agents, logging, or required security configurations.		
145.	The bidder should ensure full-context risk correlation by combining vulnerability data, threat, identity exposure, asset value, and configuration risks.		

2/1/c

146.	It is preferable that the solution should be support integration with Endpoint Detection and Response (EDR) and Endpoint Protection Platforms (EPP) for enhanced endpoint visibility and containment capabilities.		
147.	The bidder should provide identity risk monitoring capabilities, including correlation of user permissions, privileged access, and detection of anomalous or risky identity behavior.		
148.	This Attack Surface Management (ASM) features should be capable to deal 25 exposed IPs that may be different from external IPs mentation in VA for web application.		
149.	The connector should be installed in the same physical server used for VA solution.		
150.	The connector / feature should be installed in industry standard VM environment.		
149.	The solution should support proprietary operating system considering the best practice used by the same industry		

Table: Training

Item	*Question / Requirement*	*Bidder Response*
1.	The vendor/supplier must provide on-premises local training for 03 personnel, conducted over the necessary number of days, to ensure the efficient operation of the offered solution.	