

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021					
Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
1	30	Eligibility Criteria	Bidder must not be an existing System Integrator (SI) managing Bank's Data Centre (DC) and Disaster recovery (DR) site.	Request to relax this point	No change in the clause
2	65	Technical specs Point 2	The Solution should be able to perform agentless and agent-based scanning.	Requesting to change "The Solution should be able to perform agentless or agent-based scanning."	No change in the clause
3	65	Technical specs Point 5	The Solution must be able to carry out patch auditing for a) Endpoints/Servers/Laptops/PCs (Windows & Non-Windows) b) Networking devices & IOTs c) All types of Databases d) Systems hosted on clouds and VMs e) Internal Web applications	Requesting to provide the following information: 1. How many IOT devices/IPs? 2. How many web-apps? 3. What is the nature of VA that have to be performed on the web-applications? 4. What all types of authentication mechanism should be supported by the VA tool to perform authenticated-scan on the web-application? 5. What are the different technology/programming-languages have to be supported by the VA tool for scanning the web-application? 6. Are there any API within the web-application and if yes then will these APIs also has to be considered under the VA scope? 7. Please provide list of databases and their versions that will be under the scanning scope?	The details will be shared to the successful bidder

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
4	67	Technical specs Point 4	The reports generated should have option to encrypt and password-protected.	Requesting to remove this point as it is OEM proprietary Specs. Requesting to change from "The reports generated should have option to encrypt and password-protected" to "Report generated should have restricted access to specific users"	Refer Addendum 1
5	67	Technical specs Point 7	The Solution should have an option of defining the data retention period so to retain results for a defined and configurable period of time after which the results are expired and archived into another quarriable database automatically.	Requesting to remove this point as it is OEM proprietary Specs.	No change in the clause
6	67	Technical specs Point 8	The Solution should provide views of active and mitigated vulnerabilities with automatic migration of vulnerabilities from active to mitigate when closed, flag re-opened vulnerabilities with recurrence count.	Requesting to please provide confirmation if this requirement can be addressed with IT ticketing system.	No change in the clause
7	67	Technical specs Point 12	The Solution should be able to track mitigation for the reported findings of scanning and assessment activities, maintain comprehensive dashboard of the same.	Requesting to confirm if the dashboard (with Metadata) can be manage on the cloud.	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
8	67	Technical specs Point 16	Solution must provide regulatory compliance related scanning & reports for compliance requirements not limited to PCI DSS/ISO 27001/GDPR/SOC2/MAS/HKMA etc.	Requesting to provide additional details as as there are few compliances that simply mandate that Vulnerability Scanning / Risk Assessment has to be done. Nothing else in regards to actual hardening configurations or otherwise. So what is the ask from the Bank over here? Please provide the compliance requirement in detail. Other VM OEMs offering this template is simply renaming a standard vulnerability scan template in order to appear bespoke to GLBA / HKMA requirement.	No change in the clause
9	68	Technical specs Point 2	The Solution must support the following minimum alerting types out of the box: a) SMTP/Mail b) SMS c) SNMP d) Syslog	Requesting to remove "SMS Alerting" as it is OEM proprietary Specs.	No change in the clause
10	68	Technical specs Point 3	The Solution should provide an option of uploading and verifying the custom audit files/ Secure Configuration Documents (SCD) to meet Banks benchmark requirements for compliance. SCDs may be in the form of pdf/csv etc.	Requesting to change this spec to "The Solution should provide an option of uploading/reading and verifying the custom audit files/ Secure Configuration Documents (SCD) to meet Banks benchmark requirements for compliance. SCDs may be in the form of pdf/csv etc (if the tool is going to read the configuration then no need of specific format support)"	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
11	68	Technical specs Point 4	The Solution must provide reputation and threat intelligence feeds from OEM & min. three more reputed renowned service providers for malware, botnet discovery, IOCs etc with recommendations/contextualization which can be included in the scanning profile.	Requesting to confirm if the ask is for vulnerability Management solution or end point security solution. Assuming this feature is expected in VM solution then why limiting only to malware/Botnet discovery on signature basis and why not include sandboxing for malware and botnet to identify zero-day malware/botnet.	Refer Addendum 1
12	69	Technical specs Point 7	Support availability in India (Mumbai & Hyderabad)	Requesting to change to "24x7 support availability from OEM by email/remote"	Refer Addendum 1
13	69	Technical specs Point 1	The Solution's license should be IP/Asset based and perpetual in nature. Perpetual would mean that Bank shall be able to utilize the functionality of the product after expiry of license however product update and software would not be available if license is not renewed.		No change in the clause
14	65	Technical specs Point 4	The solution should be able to complete scan within 3 hrs (approximately) for 300 servers.	Can be done provided the servers have good connectivity and not running too many services. The VM also needs to have more than the recommended specs.	No change in the clause
15	66	Technical specs Point 5	The Solution must be able to carry out patch auditing for: a) Endpoints/Servers/Laptops/PCs (Windows & Non-Windows) b) Networking devices & IOTs c) All types of Databases d) Systems hosted on clouds and VMs e) Internal Web applications	Change Request: Remove this point as it is OEM Proprietary Spec. 5(a) Endpoints/Servers/Laptops/PCs (Windows or Non-Windows)	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
16			The Solution should track DHCP changes by associating scan results with system hostnames or other parameters.	Tracking done only if scanned via hostname since our licence is tied to IPs consumed	No change in the clause
17			The Solution should have an option of defining the data retention period so to retain results for a defined and configurable period of time after which the results are expired and archived into another quarriable database automatically.	Data is retained indefinitely so this is not really an issue.	No change in the clause
18			Solution must provide regulatory compliance related scanning & reports for compliance requirements not limited to PCI DSS/ISO 27001/GDPR/SOC2/MAS/HKMA etc.	We have most of the compliance templates. We can add if they need more.	No change in the clause
19			The Solution must support the following minimum alerting types out of the box: a) SMTP/Mail b) SMS c) SNMP d) Syslog	For SMS alert mechanism, Bank needs to provide SMS Gateway	No change in the clause
20			The Solution must provide reputation and threat intelligence feeds from OEM & min. three more reputed renowned service providers for malware, botnet discovery, IOCs etc with recommendations/contextualization which can be included in the scanning profile.	Since data requested for malware, botnet discovery, IOCs etc are part of EDR, Malware Analysis or APT solutions, hence request you to please remove this Point / Specification	Refer Addendum 1

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
21			Solution must provide OEM-certified two L2 resources onsite for continuous management & operations	Yes, via our partner. There will be a separate cost for this	Refer Addendum 1
22			The vendor should be minimum NIAP/Common Criteria (CC) EAL or any industry Security standards certified in valid condition.	Not sure about certification. However, our scanning engine is certified and approved by PCI Council for ASV scans.	No change in the clause
23	65	Vulnerability Assessment (VA) Scanning ,2	The Solution should be able to perform agentless and agent-based scanning.	Agent/Agentless Scanning needs to be on prem? Kindly confirm	On premise & off premise scanning is required. However, scanning engine & data should be on premise
24	65	Vulnerability Assessment (VA) Scanning,3	The Solution must be capable to perform unauthenticated or authenticated i.e., credential and non-credential-based VA of all entire IT Infrastructure"	Please mention which tool Bank is using for authentication and does Bank want to achieve automation in authentication. Please confirm	Will be shared with the successful bidder
25	65	4	The solution should be able to complete scan within 3 hrs (approximately) for 300 servers.	On what basis Bank has achieved this number, Please clarify Time taken for scanning an asset depends on the configuration, data residing, application running and multiple other factors. Time taken for a asset may be less than compared to another. So to give an estimation of scanning depends on various factors and may vary from asset to asset	It is approximate taken from the existing environment.

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
26	65	Vulnerability Assessment (VA) Scanning ,5	The Solution must be able to carry out patch auditing for a) Endpoints/Servers/Laptops/PCs (Windows & Non-Windows) b) Networking devices & IOTs c) All types of Databases d) Systems hosted on clouds and VMs e) Internal Web applications	Please share the list of databases used in Bank.	Will be shared with the successful bidder
27	66	7	The Solution should support automatic scanning for specific vulnerabilities/IOCs and browse the vulnerability database by category and type	Please elaborate and explain what Banks want to achieve from this clause	This functionality is required for proactive vulnerability mangement
28	66	2	The Solution should be able to create multiple scanning profiles based on department, asset type, platforms, users, geographies, network zones, applications etc	Profile creation on Geography: Please suggest/elaborate what is Banks expectation in terms of geographic profiling	Bank is having global presence.Hence,geographic profiling is required
29	66	Vulnerability Management (VM) & Analysis ,4	The Solution should have lowest false positive rate along with accuracy and efficiency through validation process	Please define what is the lowest false positivity rate which is acceptable to Bank	Bidder is expected to have least false positivity rate (< 2%)

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
30	67	Dashboard & Reports,4	The reports generated should have option to encrypt and password-protected	<p>This clause represents that Bank can manually encrypt or add a password to the reports generated from the solution. Kindly confirm</p> <p>Reports generated are in different formats and can be downloaded from the console. To add encryption or password protection Bank needs to have tools to do the same</p>	Refer Addendum 1
31	67	Dashboard & Reports,7	The Solution should have an option of defining the data retention period so to retain results for a defined and configurable period of time after which the results are expired and archived into another quarriable database automatically	"quarriable into another database " please elaborate and explain the clause	Required for the purpose of archival and retention
32	68	Integration,1	The Solution should provide mechanism to integrate through open API/web services or other mechanism: a) AD b) SIEM c) PIM (Perform secure credential-based VA) d) ITGRC e) Ticketing tool and workflow systems	Please share the OEM details of the solutions required to be integrated	Will be shared with the successful bidder

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
33	68	4	The Solution must provide reputation and threat intelligence feeds from OEM & min. three more reputed renowned service providers for malware, botnet discovery, IOCs etc with recommendations/contextualization which can be included in the scanning profile.	This clause should be removed from the RFP as this point is more specific to Threat Intel solution. VM provides vulnerability based intel and reputation and not for malware, botnet IOCs etc.	Refer Addendum 1
34	58	z	Dashboard should have Role based as well as Discretionary access control facility to restrict access to vulnerability scans based on user security clearance level.	Please clarify what you mean by " Discretionary access control facility to restrict access to vulnerability scans based on user security clearance level."	User and Role based restriction
35	58	6. General Scope of Work u	The selected bidder has to supply, install and configure the hardware and software provided as per the timelines and SLA levels prescribed in the RFP document.	Request Bank to confirm if we need to factor the Hardware Cost also? If Not,Kindly confirm apart from solution what other components need to be factored.	Bank will provide Virtual Machines with OS .All required configuration to be taken by the selected bidder
36	61	11.2 Implementation,c	Installation and configuration of hardware and related software and its components, integration with AD, SIEM, PIM & ITGRC solution should be completed within -8- weeks of issuance of purchase order.	Request Bank to amend the clause as "Installation and configuration of hardware and related software and its components, integration with AD, SIEM, PIM & ITGRC solution should be completed within -8- weeks from the date of delivery of the software componets"	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
37	71	21. Payment Terms ,Annexure -12	1) 50% of the Software / Application license cost on delivery of Software / Application Licenses plus 100% of VAT / CST & Octroi / entry tax (wherever applicable) at actuals. 2) 30% of the Software / Application license cost after successful installation of the Software / Application and payable against acceptance signoff in the form of Acceptance Report signed by both Bank’s identified Project Manager & vendor representative. 3)20% of the Software / Application license cost after Go-Live closure signoff from Bank.	Request Bank to amend the clause as below, 1) 80% of the Software / Application license cost on delivery of Software / Application Licenses plus 100% of VAT / CST & Octroi / entry tax (wherever applicable) at actuals. 2) 10% of the Software / Application license cost after successful installation of the Software / Application and payable against acceptance signoff in the form of Acceptance Report signed by both Bank’s identified Project Manager & vendor representative. 3)10% of the Software / Application license cost after Go-Live closure signoff from Bank.	No change in the clause
38	33	Technical Bid Evaluation B.a (2)	The number of implementations of proposed solution completed directly by the bidder in BFSI/ Govt. Sector in the last 3 years in India.	Kindly consider large enterprise experience also along with BFSI/Government	No change in the clause
39	91	Annex 20- Onsite Resource	Shift: One L2 level resource is required for performing shift duties i.e. resource should be available in each shift for 8 Hours a day, timings will be: ☐ 07:00 AM to 03:00 PM ; ☐ 03:00 PM to 11:00 PM ; ☐ 11:00PM to 07:00AM	Does Bank require L2 resource in all the 3 shifts ? Or only one shift per day. Kindly confirm	Refer to Annexure 20 of RFP
40	60	11 Project Time Lines	All the software components must be delivered within -4- weeks of issue of the confirm purchase order to the successful Bidder.	Kindly consider delivery period to 6-8 weeks	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
41	61	11.2 Project Time Lines	Installation and configuration of hardware and related software and its components, integration with AD, SIEM, PIM & ITGRC solution should be completed within -8-weeks of issuance of purchase order.	Kindly consider implementation & integration timeline to 10-12 weeks	No change in the clause
42	10	6	Exemption from submission of EMD and application money shall be given to bidders, who are Micro Small and Medium Enterprises (MSME) / Startups	Is EMD and Application fee exempted for Medium Enterprises under MSME.	Yes
43	11	9.1	The successful bidder shall execute a) Service Level Agreement (SLA) and Non-Disclosure Agreement (NDA) (As per Annexure 21), which contained all the services and terms and conditions of the services to be extended as detailed herein. The successful bidder shall execute the SLA and NDA and provide the same along with acceptance of Purchase Order.	Please provide SLA documents. We need to factor the same while bidding whether we can comply the SLA points.	Please refer Annexure 13 & 20 of RFP
44	11	9.2	All the expenses related to execution of the document such as the applicable stamp duty and registration charges if any shall be borne by the successful bidder.	What will be the stamp duty?	No change in the clause
45	11	11.1	Bank reserves the right to terminate this RFP at any stage without any notice or assigning any reason.	Once order is processed could not cancelled.	No change in the clause
46	71	21 (A)	Payment Terms: A) Software / Application License Cost	as per standard process, we have to pay disti/OEM in advance. Request to make 100% payment for product against delivery.	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
47	101	18	<p>Audit The Bank and its authorized representatives, including Reserve Bank of India (RBI) or any other regulator shall have the right to visit any of the Service Provider’s premises without prior notice to ensure that data provided by the Bank is not misused. The Service Provider shall cooperate with the authorized representative/s of the Bank and shall provide all information/ documents required by the Bank.</p>	<p>Request to read clause as below: “The Service Provider shall keep full, true and accurate records limited to the scope of this Agreement. To ensure compliance, the Company upon prior notice of thirty (30) days to the Service Provider may examine the records related to the Agreement. Such examination or audit of services can take place once per calender year. Any finding during the audit, shall be shared with the Service Provider and shall be discussed and agreed mutually for its closure.”</p>	No change in the clause
48	59	Annexure 12 – Project Details & Scope of Work. Section 7.g Detailed scope of Work	Selected Bidder will provide end to end Software solution to the Bank which will have the capabilities to carry out vulnerability assessments and scanning of all IT assets that is servers (windows, non-windows), Network devices, Security Devices, Endpoints (PCs, TABs and Laptops), Web applications, IoTs and etc.	Kindly provide information for following: PC : Operating System and Number of Devices TABs : Operating system and Number of Devices Web Applications : what is the scope of web application IOTs: what kind of IOTs device and number of device.	Will be shared to successful bidder
49	59	Annexure 12 – Project Details & Scope of Work. Section- 7. h - Detailed scope of Work	The selected bidder should provide VM solution to be deployed on Virtual Platform Bank will provide the required Virtual Platform resources i.e., Hardware, Operating System and Database. Bidder to provide the detailed resource requirement for the Virtual platform.	Request to kindly amend the clause as " The selected bidder should provide Hardware appliance or a VM solution to be deployed on Virtual Platform Bank will provide the required Virtual Platform resources i.e., Hardware, Operating System and Database. Bidder to provide the detailed resource requirement for the Virtual platform. "	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
50	59	Annexure 12 – Project Details & Scope of Work Section- 7. i - Detailed scope of Work	Selected bidder should provide IP/Asset based perpetual licenses for the VM Solution. The details of license requirement are mentioned in the commercial bid document.	Each OEM has their own licensing mechanism and by asking this clause bank is restricting OEM from participation. We request you to amend the point as " The Solution's license should be IP/Assest based and perpetual/subscription for the VM solution. "	No change in the clause
51	61	Annexure 12 – Project Details & Scope of Work Section no 12 - Support and Maintenance	All support by SI/OEM has to be provided onsite. Remote access will not be allowed though any remote desktop sharing applications.	OEM will provide remote support for the issue resolution/maintainance/upgrade etc... Kindly amend the clause as " All support by SI/OEM has to be provided as a combination of remote and onsite. Remote access will be allowed for OEM support team though any secured remote desktop sharing applications. "	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
52	69	Annexure 12 – Project Details & Scope of Work Section no : 15. Technical Specifications /Requirement point no VI - Licensing	The Solution's license should be IP/Asset based and perpetual in nature. Perpetual would mean that Bank shall be able to utilize the functionality of the product after expiry of license however product update and software would not be available if license is not renewed.	Each OEM has their own licensing mechanism and by asking this clause bank is restricting OEM from participation. We request you to amend the point as " The Solution's license should be IP/Assest based and perpetual/subscription in nature ".	No change in the clause
53	73	Annexure 12 – Project Details & Scope of Work section no : 23 -- Right to Alter Quantities	The Bank reserves the right to alter the requirements specified in the Tender. The Bank also reserves the right to delete one or more items from the list of items specified in the Tender. The Bank will inform all Bidders about changes, if any. The Bidder agrees that the Bank has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities	Request you to amend the clause as "The Bank reserves the right to alter the requirements specified in the Tender. The Bank also reserves the right to delete one or more items from the list of items specified in the Tender. The Bank will inform all Bidders about changes, if any. The Bidder agrees that the Bank has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be mutually discussed and agreed with the bank and then proportionately adjusted with such additions or deletions in quantities. "	No change in the clause

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
54	78	Annexure 15–Commercial Bid	The above price will remain valid for the terms of the contract.	Is this in terms of repeat order. Price will be firm for this requirement only. For any additional requirement during contract period, prices will be shared at that time only.	No change in the clause
55	57	6 (a). General Scope of work	The proposed solution must be able to operate 100% on-premises. Scan results should always be available on premise. The proposed solution should not be cloud based.	We propose BOB to evaluate Cloud VM based option as well. OEM we represent has services hosted on MeitY approved data centres in India. Complete data will remain in India. Kindly consider both On-Premise as well as cloud VM solution	No change in the clause
56	30	Financial 1B	<p>The Bidder must have registered an average turnover of Rs. 50 Crores (from Indian Operations only) during the last three completed financial years (FY) i.e. 2018-19, 2019-20 and 2020-21 (Not inclusive of the turnover of associate companies).</p> <p>In case if audited financials for FY 2020-21 is not available, then the bidder may submit financials for FY 2017-18, 2018-19 and 2019-20.</p>	Exempted for MSME certificate are there	Exemption will be provided as per extant guidelines of GOI
57	33	a Presentation cum Interview	Bidder to provide presentation on the proposed solution and implementation methodology	Presentation submit with online bid or separately	Live presentation to be given to the committee and ppt & methodology to be submitted

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
58	91	Annex 20 Onsite Resource Requirement	Onsite resource will come in shift duty (one shift per day) as per above timings as per requirement of VA scanning & management as decided by Bank team. Resources have to work as per the above shift timings on all days during the contract period including public holidays, Saturdays & Sundays.	When will be week offday	Shall be finalised with successful bidder
59	69	4 Sizing, Support & Deployment	Solution must provide OEM-certified two L2 resources onsite for continuous management & operations	(In full tender document there is only mention one L2 resources) but in this Two L2 resources mention Please confirm	Refer Addendum 1
60	72	ATS/AMC	Payable yearly in advance against receipt of satisfactory service report of previous year from the Bank's Project / Operation Manager.	We assume that first year payment also in advance please confirm	No change in the clause
61	78	3	No. of Units - 5000	Please clarify locations covering 5,000 IP addresses. Whether this covers assets in data center or also branch locations and end-user devices .	Will be shared with the successful bidder

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
62	61	11.4	<p>Three training are to be provided for the banks team during the contract period of 3 years.</p> <p>I. First traing during the implementation of VM solution on mutually agreed dates.</p> <p>II. Second training after completion of implementation of VM solution during handing over to operations team and this should be the OEM certified training.</p> <p>III. Third training will be post-handover to operations team. Dates as decided by the Bank team.</p>	<p>1. Please confirm the understanding that there will be only 1 set of training for the project duration of 3 years.</p> <p>2. Please mention the number of attendees from Bank side for each of the 3 trainings.</p> <p>3. Please elaborate on the second training wherein Bank has requested for OEM certified training. What is expctation of the Bank from the Bidder w.r.t. the OEM Certified training?</p> <p>4. Please confirm the understanding that all the 3 training will be conducted at Bank's premises at Hyderabad.</p>	<p>1. 3 set of trainings as per RFP Annexure 12 para 11</p> <p>2. No of participants will be 5 to 6.</p> <p>3. OEM Certified training to be provided by the OEM along with certification.</p> <p>4. Mode of training and location can be decided mutually with the selected bidder</p>
63	92		SLA & NDA Format	Please confirm that the SAL & NDA format is only applicable to the successful bidder and will be executed at the time of contract signing.	No change in the clause
64	65	5	<p>The Solution must be able to carry out patch auditing for</p> <p>a) Endpoints/Servers/Laptops/PCs (Windows & Non-Windows)</p> <p>b) Networking devices & IOTs</p> <p>c) All types of Databases</p> <p>d) Systems hosted on clouds and VMs</p> <p>e) Internal Web applications</p>	Please share the list of databses used in Bank.	Will be shared to successful bidder

PRE-BID Query response - Vulnerability Management (VM) Solution RFP Ref:BCC:CISO:113:557 DATED 20.08.2021

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Queries	Bank Clarification
65	31	D 1.	The proposed Solution must be implemented in at least two Commercial Banks / Financial Institutions in India in last 3 financial years in India.	The proposed Solution must be implemented in at least one Commercial Banks / Financial Institutions in India in last 3 financial years in India.	No change in the clause