



Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

Clarification of Pre Bid Queries: Request for Proposal (RFP) For Selection of Service Provider for Conducting Red Team Exercise

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
1	10	Section 2	The purpose of enabling Punjab national Bank ("the Bank") to select Service Provider for conducting Red Team Exercise for the Bank as per the scope of work given in this RFP.	Please confirm whether the Bidder has to perform the Red teaming exercise from PNB's site or it can do that remotely	The activity to be performed at PNB Premises.
2	10	Section 2	The purpose of enabling Punjab national Bank ("the Bank") to select Service Provider for conducting Red Team Exercise for the Bank as per the scope of work given in this RFP.	Is Red Team Assessment need to be perform physically / onsite at Global Location, please confirm along with location details?	Red Team Assessment need to be perform physically at PNB premises Delhi and Mumbai.
3	11	Section 3.1 Point B	The Platform should support scaling up to national and remote networks.	Please confirm the count of locations and whether these are on prem or at cloud	On premise
4	11	Section 3.1 Point H	The platform should support integration with vulnerability management and it should also be able to detect the vulnerabilities which can be exploited	Please confirm which Vulnerability management solution is deployed at PNB's site	Nessus

5	12	Section 3.1 Point I	The Platform should support several integrations out of the box, namely to SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, and furthermore also provides an open API that vulnerability management platforms can connect to either directly or via an orchestration and automation platform	Please provide the details of SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, need to be integrated with Red Teaming Platform	Will be shared with the successful bidder
6	12	Section 3.4	The vendor shall be responsible for delivering social engineering exercises every quarter for a year	Please confirm whether this activity is expected only for 1 year not for 2 years	2 Years
7	NA	NA	NA	Details of currently implemented Red Team platform, if exist and PNB want to continue with the same?	No Platform Present.
8	12	Section 3.4	The vendor shall be responsible for delivering social engineering exercises every quarter for a year	Approx. Count of Users for “Social Engineering” Activity?	All Employees
9	12	Section 3.3	Training- Vendor is required to impart training to the identified bank personnel/ SOC team on the platform, functionality and services. In addition to that, mandatory training of at least 2 Days is to be provided to Bank staff (10 officials) twice in the first year of Contract (at a minimum gap of 6 months), with complete knowledge transfer for handling the guidance as Blue team against Red Team Exercise	Please confirm whether this training can be given online to the Bank staff	Please be guided as per RFP.

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
10	10	Scope of Work 3.1 d	This imported data has to be stored in the test / attack library for replay at any time.	Kindly remove this clause. PCAP data is an action and sequence of events and this cannot be converted into a test/attack library for replay. The clause can be changed to " Should have the ability to create customized test cases on the basis of PCAP data captured"	Please be guided as per RFP.
11	10	Scope of Work 3.1 i	The platform shouldn't just test endpoint security controls, it also should test the performance of network security controls (like firewalls, proxies, IDS/IPS).	This clause may be modified as this tool is for Security test case determination. Performance parameters are different and hence kindly do not include performance parameters in the same.	Please refer Corrigendum-1, Sr no -3
12		Scope of work Section 3	addiional Clause	Kindly include the following clause " PNB SOC team should be able to create their own customized testing simulation environment using simple drag and drop feature." <u>Justification</u> This is a very important clause as changing dynamics of attacks require PNB SOC team to have their own simulation environment very easily	Please be guided as per RFP.

13		Scope of work Section 3	additional Clause	<p>Kindly include the following clause "</p> <p>While performing training exercises for the PNB SOC team using this tool, then each participant should be assigned a designated role , for eg. SOC analyst, firewall administrator, linux forensics. The roles should be displayed throughout the exercise so as to provide better visibility of learning outcomes".</p> <p><u>Justification</u> - Without this function the Environment will not be complete and will not help fulfil the need for continuous improvement of the PNB SOC team</p>	Please be guided as per RFP.
14		Scope of work Section 3	addiional Clause	<p>Kindly include the following clause “</p> <p>PNB SOC team should be able to choose appropriate Role based access to the tool such that they can chose between a simulation exercise or a learning exercise. There should be separate environment for both the use cases and historical data will be stored for minimum of six months"</p> <p><u>Justification</u> - This clause is extremely important as the platform should offer both simulation and also continuous learning for the PNB SOC team such that all the attacks can be tried out in their environment with least impact and best results.</p>	Please be guided as per RFP.

15		Scope of work Section 3	additional Clause	<p>Kindly include the following clause "</p> <p>The tool should offer a continuous improvement platform for PNB Security team on specific areas like Firewall, SOC, Forensics, OS and hence should offer specific filtered out reports from the learning exercises. These reports should be filtered based on individuals, groups, attack types</p> <p><u>Justification</u> : Reporting function for learning and simulation is extremely important as without that the function curve is not complete.</p>	Please be guided as per RFP.
16	9	For On-Premise based Red Team capability solution	The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs to perform below activities	<p>Is the bidder expected to provide all hardware, software , etc for the entire solution to be deployed on premise? Kindly clarify?</p> <p>Wil PNB Provide the hardware necessary for the solution along with system software in the PNB premises?</p>	All requisite Hardware & Softwares for performing Red team Exercise has to bring by vendor.
17	9	For On-Premise based Red Team capability solution	The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs to perform below activities	Is the bidder expected to Simulate the PNB Data center and Application solution? If yes, kindly give an indication of the number of technologies and sizing of the VM that needs to be provisioned for the tool.	Please be guided as per RFP.
18	9	For On-Premise based Red Team capability solution	The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs to perform below activities	<p>If the bidder is expected to simulate the PNB Data center or part of it?</p> <p>If yes, Who is going to provide the license of the same, like firewall, etc. Kindly clarify.</p>	Please be guided as per RFP.

19		3.4 Social Engineering (h)		There is no mention of the total number of users for which social engineering simulation needs to be done. We need this as the licensing is based on number of users being enabled for simulation	All Employees. However, each exercise will be limited to 10,000 employees.
20	31	26. Patent Rights	The Supplier shall grant to the Bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including all inventions, designs and marks embodied therein in perpetuity.	The bidder needs to provide licensed software for the components On premise Red Teaming platform and social engineering. Bidder cannot offer this as only service but rather licensed software has to be provided. Is our understanding correct?	Please be guided as per RFP.

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
21	26	2. DURATION OF CONTRACT	The contract will be valid for two years from the date of agreement signed with the Bank, if not revised earlier of all the hardware & software licenses. Bank at its sole discretion may extend the contract for a further period of 1 year or any other period, at the same rate and same terms & conditions, subject to satisfactory performance of successful bidder and mutual agreement on the terms and conditions. Bank reserves right to cancel the contract at any time in case system fails to meet any of the requirements as mentioned in the RFP.	Bidder requests Bank to kindly allow full commitment on the entire Tenure of 2 Years. Bidder requests Bank to remove the clause on Termination Rights within the Contract Term.	Please be guided as per RFP.
22	27	9. PAYMENT	The invoices shall be raised after completing the whole round of Red Team Exercise as per scope of work mentioned	Bidder understands that the Bank will perform one round of Red Team Exercise every quarter. The Invoices	Please be guided as per RFP.

			<p>in the RFP and payment shall be released within 30 days from the receipt of undisputed invoices by bank. In case of any dispute regarding the invoice will be communicated to the selected bidder within 15 working days from the date of receipt of the invoice.</p> <p>Further, the above payments will be released only after submission of PBG and signing of SLA (including Do & Don't), IP and NDA by Successful Bidder.</p>	<p>shall be raised post completion of the Quarterly Red Team Exercise and Payment should be made by the Bank within 30 days of Invoice generation. This cycle would repeat every quarter.</p>	
23	30	20. TERMINATION OF CONTRACT	<p>The quality of services given by the bidder & progress of the project will be reviewed monthly and if the services are not found satisfactory, the Bank reserves the right to terminate the contract by giving 30 days' notice to the bidder, including 15 days curing period. The decision of the Bank regarding quality of services shall be final and binding on the bidder.</p>	<p>Bidder requests Bank to kindly allow full commitment on the entire Tenure of 2 Years. Bidder requests Bank to remove the clause on Termination Rights within the Contract Term.</p>	<p>Please be guided as per RFP.</p>
24	44	Annexure-X (8)	<p>Bank may place Orders for any item as and when required during the entire contract period at the unit rates finalized after Reverse Auction. Bank is not bound to place any minimum order. The quantity will also be as per requirement</p>	<p>Bidder requests clarification on this point. Basis the RFP document, the Scope of Work would be to do one Red Team Exercise every Quarter.</p>	<p>Please be guided as per RFP.</p>
25	10	3. SCOPE OF WORK	<p>a. The Platform impact on network performance should be minimal during Red Team Exercise. The Platform should not process actual live traffic and so should not impact any user flows. Non-Destructive simulation Initiator would only be allowed to generate lightweight traffic. Tests in the production network should not be destructive (i.e. are only transport, not execution) - destructive behaviour tests are only done in the secure containers, a</p>	<p>Bank to confirm whether the Sandbox environment is already available in the infra or Bidder shall consider in the solution.</p>	<p>Bidder has to provision the same.</p>

			sandbox separated from the production network. Most network tests should be measured in hundreds of Kilobytes, which is very small.		
26	11	3. SCOPE OF WORK	b. The Platform should support scaling up to national and remote networks. If need be it should support PNB's International (Global) Locations as well.	Bidder requests Bank to confirm the following points - - Type of connectivity at these locations. - Connectivity between these locations. - Total number of locations (Remote & Global). - SANDBOX availability at these locations (Remote & Global).	Will be shared with the successful bidder
27	12	3. SCOPE OF WORK	h. The platform should support integration with vulnerability management and it should also be able to detect the vulnerabilities which can be exploited.	Bidder requests Bank to confirm the make & model of existing VA tool.	Nessus.
28	13	3. SCOPE OF WORK	i. The Platform should support several integrations out of the box, namely to SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, and furthermore also provides an open API that vulnerability management platforms can connect to either directly or via an orchestration and automation platform. The platform should support vulnerability prioritization based on simulation score. The platform shouldn't just test endpoint security controls, it also should test the performance of network security controls (like firewalls, proxies, IDS/IPS). This means that test results need to be interpreted in context. As an example, maybe a server has an identified	Bidder request Bank to confirm the make & model of the mentioned tools like SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints.	Will be shared with the successful bidder

			vulnerability, but tests should show that either (or both) the endpoint and the firewall actively detect and block the corresponding exploit. This could significantly lower the criticality of the vulnerability. As a result, the platform provides the ability for users to tag actions so that corresponding results can then be highlighted in reporting.		
29	14	3. SCOPE OF WORK	3.2. The bidder shall develop a Project Management Plan which shall address the following Service(s) processes: - Document Control - Change Management - Inspection and Testing	Bank to confirm the bidder scope w.r.t. Change Management.	Please be guided as per RFP.
30	15	3. SCOPE OF WORK	The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs to perform below activities	Bank to confirm on Hardware required to deploy the solution. Will Bank provide the required hardware or bidder to provide?	All requisite Hardware & Softwares for performing Red team Exercise has to bring by vendor.
31	16	3.4 Social Engineering	The vendor shall be responsible for delivering social engineering exercises every quarter for a year and should be able to capture statistics to measure success of exercise.	Does Bank expect to implement the on-prem solution for Phishing simulation? Or Can Phishing simulation be delivered as a Service model?	On-Premise

32	17	3.4 Social Engineering	<p>b) Vendor should be able to perform email and phone based social engineering campaigns</p> <p>c) Vendor using social engineering should be able to harvest bank's employees credentials</p>	<p>Can Bidder sample the number of employees for phone based social engineering?</p> <p>How many employees need to be covered under mail Phishing simulation?</p> <p>What is the frequency of Mail and Phone based social engineering campaigns?</p>	<p>All employees need to be covered under mail Phishing simulation. However, each exercise will be limited to 10,000 employees.</p> <p>Frequency of Mail and Phone based social engineering campaigns shall be quarterly.</p>
33	18	3.4 Social Engineering	The solution should have support multilingual languages for creating phishing scenarios	Which are the languages expected to cover?	Please be guided as per RFP.
34	19	3.5 Red Team Assessment	The vendor is required to deliver Red Team assessment objectives required by Bank.	Can this activity be conducted/delivered from remotely?	The activity to be performed at PNB Premises.
35	20	Other conditions:	Bank reserves right to cancel the contract at any time in case system fails to meet any of the requirements as mentioned in the RFP.	This will not be applicable on the solution implemented at Bank site for Red Teaming/Social Engg. Need confirmation from bank on this.	Please be guided as per RFP.
36	21	ELIGIBILITY CRITERIA OF THE BIDDER	Banks existing vendors will not be allowed to participate in this RFP	If bidder is a existing vendor, then the team allocated for RED team excersice activity should not be same or dependent to the team who supports for the existing serivces for PNB.	Please be guided as per RFP.

37	14		Other conditions: a. Bank reserves right to cancel the contract at any time in case system fails to meet any of the requirements as mentioned in the RFP.	In case of any termination, the Bank shall provide a notice period of 90 days and shall be liable to pay early termination charges equivalent to the remainder of total contract value and/or applicable penalties.	Please be guided as per RFP.
38	27	7	RED TEAM EXERCISE TIME Bidder shall have to complete Red Team Exercise within 6 weeks from start of every quarter and shall submit reports within 1 week of completion of Red Team Exercise as per scope of the RFP.	Bidder requests Customer to change the Red Team Exercise completion period to 8 weeks and the report submission period to 2 weeks (from date of completion of Red Team Exercise).	Please be guided as per RFP.
39	29	17	DELAYS IN THE SUPPLIER'S PERFORMANCE Delivery of the goods and performance of the Services shall be made by the supplier in accordance with the time schedule specified by purchaser. Any delay in performing the obligation by the supplier will result in imposition of liquidated damages and/or termination of contract for default.	The delay in Supplier's performance is included above 'Penalty' clause. For the termination of contract, the delay shall be more than 30 days for a the material requirement. Clause to be modified accordingly.	Please be guided as per RFP.

40	30	18	<p>INDEMNITY</p> <p>The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes (except GST) and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidder's obligation under these general conditions or for which the bidder has assumed responsibilities under the purchase contract including those imposed under any contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed by the bidder or bidders in connection with the performance of any system covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to conform and effectuate the purchase contract and to protect the Bank during the tenure of purchase order. Where any patent, trade mark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liable for settling with such third party and paying any license fee, royalty and/ or compensation thereon.</p> <p>In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the machine supplied by the</p>	<p>The bidder shall not be liable for any indirect, incidental, special, consequential a, exemplary or punitive damages. Furthermore, for the services being provided by the Supplier, IP infringement clause/indemnity is not applicable. Therefore the IP infringement liability should be capped to the total contract value. Request the clause to be modified accordingly.</p>	<p>Please be guided as per RFP.</p>
----	----	----	---	---	-------------------------------------

			bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidder's cost against such third party's claim and / or actions and against any law suits of any kind initiated against the Bank. Successful bidder (successful bidder) will also assume full responsibility of any loss or damage caused due to any of their onsite engineer/representative.		
41	30	20. TERMINATION OF CONTRACT	<p>TERMINATION OF CONTRACT</p> <p>The quality of services given by the bidder & progress of the project will be reviewed monthly and if the services are not found satisfactory, the Bank reserves the right to terminate the contract by giving 30 days' notice to the bidder, including 15 days curing period. The decision of the Bank regarding quality of services shall be final and binding on the bidder. The Bank shall have the right to terminate/cancel the contract with the selected bidder at any time during the contract period, by giving a written notice of 30 days, for any valid reason, including but not limited to the following:</p> <ul style="list-style-type: none"> a. Excessive delay in execution of order placed by the Bank b. Discrepancies / deviations in the agreed processes and/or products c. Failure of successful bidder (successful 	<p>Bidder proposes a fixed 2 year contract and payment of early termination charges in case of any pre mature termination. The right to cancel the contract shall be only in the event a material obligation or a material requirement is not fulfilled by the bidder.</p> <p>Bidder proposes that the termination notice period should be minimum 90 days and the curing period should be minimum 30 days.</p>	Please be guided as per RFP.

			<p>bidder) to complete implementation of solution within the time as specified in the RFP document</p> <p>d. Violation of terms & conditions stipulated in this RFP.</p> <p>e. If the service provided is not satisfactory on the objectives as specified in the RFP are not achieved.</p> <p>f. Penalty as in clause 11 reaches its max. limit.</p> <p>Notwithstanding anything contained hereinabove, the Bank reserves the right to terminate the contract at any time without assigning any reasons.</p> <p>In case of termination of contract for the reasons that the services of successful bidder are not found satisfactory”, the Bank shall be free to Blacklist the successful bidder thereby debarring them from participating in future Bids/Tender processes.</p>		
42	31		<p>PATENT RIGHTS</p> <p>The supplier shall indemnify the Purchaser against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.</p> <p>q The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.</p> <p>q The supplier shall expeditiously extinguish any such claims and shall have</p>	<p>As stated above, IP infringement is not applicable to the services being provided by the Supplier. Therefore, the IP infringement indemnity should be capped to the total contract value. Request the clause to be modified accordingly or deleted.</p>	<p>Please be guided as per RFP.</p>

			<p>full rights to defend it there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible including all expenses and court and legal fees.</p> <p>q The Bank will give notice to the Supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.</p> <p>The Supplier shall grant to the Bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including all inventions, designs and marks embodied therein in perpetuity.</p>		
43	32	30	<p>LIMITATION OF LIABILITY</p> <p>Successful bidder's aggregate liability under the contract shall be limited to a maximum of the contract value. This limit shall not apply to third party claims for</p> <p>a) IP Infringement indemnity</p> <p>b) Bodily injury (including Death) and damage to real property and tangible property caused by successful bidder/s' gross negligence. For the purpose for the section, contract value at any given point of time, means the aggregate value of the purchase orders placed by Bank on the successful bidder that gave rise to claim, under this tender. Successful bidder shall not be liable for any indirect, consequential, incidental or special</p>	<p>We can accept unlimited liability for bodily injury (including Death) and damage to real property and tangible property caused by successful bidder/s' gross negligence. However, since , IPR infringement is not applicable to the services being provided by the Supplier, the IP infringement indemnity should be capped to the total contract value. However, Request the clause to be modified accordingly or deleted.</p>	<p>Please be guided as per RFP.</p>

			damages under the agreement/ purchase order.		
44	35	Annexure III	ELIGIBILITY CRITERIA OF THE BIDDER - Banks existing vendors who are auditors, security Integrators, Network integrators as on bid submission date will not be allowed to participate in this RFP.	If bidder is a existing vendor, then the team allocated for RED team excersice activity should not be same or dependent to the team who supports for the existing services for PNB.	Please refer to Corrigendum-1,Sr no -1
45	49	Annexure XI	Independent External Monitor (9)	Generally we don't accept Audit rights of the customers. If this clause is accepted the responsibility shall rest with the Product team and the business unit.	Please be guided as per RFP.
46	26	2. DURATION OF CONTRACT	The contract will be valid for two years from the date of agreement signed with the Bank, if not revised earlier of all the hardware & software licenses. Bank at its sole discretion may extend the contract for a further period of 1 year or any other period, at the same rate and same terms & conditions, subject to satisfactory performance of successful bidder and mutual agreement on the terms and conditions. Bank reserves right to cancel the contract	Bidder proposes a fixed 2 year contract and payment of early termination charges in case of any pre mature termination. The right to cancel the contract shall be only in the event a material obligation or a material requirement is not fulfilled by the bidder. A seperate / dedicated support desk required for Red Teaming Excersice	Please be guided as per RFP.

			at any time in case system fails to meet any of the requirements as mentioned in the RFP.		
47	27	9. PAYMENT	<p>The invoices shall be raised after completing the whole round of Red Team Exercise as per scope of work mentioned in the RFP and payment shall be released within 30 days from the receipt of undisputed invoices by bank. In case of any dispute regarding the invoice will be communicated to the selected bidder within 15 working days from the date of receipt of the invoice.</p> <p>Further, the above payments will be released only after submission of PBG and signing of SLA (including Do & Don't), IP and NDA by Successful Bidder.</p>	Bidder understands that the Bank will perform one round of Red Team Exercise every quarter. The Invoices shall be raised post completion of the Quarterly Red Team Exercise and Payment should be made by the Bank within 30 days of Invoice generation. This cycle would repeat every quarter.	Please be guided as per RFP.
48	44	Annexure-X (8)	Bank may place Orders for any item as and when required during the entire contract period at the unit rates finalized after Reverse Auction. Bank is not bound to place any minimum order. The quantity will also be as per requirement	Bidder requests clarification on this point. Basis the RFP document, the Scope of Work would be to do one Red Team Exercise every Quarter.	Please be guided as per RFP.
49		3.1.a	The Platform impact on network performance should be minimal during Red Team Exercise. The Platform should not process actual live traffic and so should not impact any user flows. Non-Destructive	The impact will be less, however the platform performs with real and live traffic. The emulation is controlled emulation, so no real damage will be done to the system. This exercise	Bidder has to provision the same.

			simulation Initiator would only be allowed to generate lightweight traffic. Tests in the production network should not be destructive (i.e. are only transport, not execution) - destructive behaviour tests are only done in the secure containers, a sandbox separated from the production network. Most network tests should be measured in hundreds of Kilobytes, which is very small.	should be done in a sandbox network environment with similar configuration as the original network.	
50		3.1.c	The Platform should support attack replay & attack import from PCAP.	The platform performs real emulations of the software and cannot handle pcap import attacks	Please be guided as per RFP.
51		3.1.d	The Platform should allow for the user creation of custom test / attack content. Such as the ability to import PCAP via a simple “click and drag” wizard. This imported data has to be stored in the test / attack library for replay at any time.	The platform allows to create mix and match, but cannot create new attacks directly by the customer, cyberange will support from backend if any new attacks needed to be created	Please be guided as per RFP.
52		3.1.g	g. Banks’ Team should also have control to create non-destructive attacks directly from the GUI. Non-Destructive Attack creation should be automated by using the platform REST API	as said in the before point, customer cannot create his own attack, but can create a flow from the given list of techniques.	Please be guided as per RFP.
53		3.1.h	h. The platform should support integration with vulnerability management and it should also be able to detect the vulnerabilities which can be exploited.	The platform is offered as an independent SOC validation tool.	Please be guided as per RFP.
54		3.1.i	The Platform should support several integrations out of the box, namely to SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, and furthermore also provides an open API that vulnerability management platforms can connect to either directly or via an	The platform is offered as an independent SOC validation tool.	Please be guided as per RFP.

			orchestration and automation platform. The platform should support vulnerability prioritization based on simulation score. The platform shouldn't just test endpoint security controls, it also should test the performance of network security controls (like firewalls, proxies, IDS/IPS). This means that test results need to be interpreted in context. As an example, maybe a server has an identified vulnerability, but tests should show that either (or both) the endpoint and the firewall actively detect and block the corresponding exploit. This could significantly lower the criticality of the vulnerability. As a result, the platform provides the ability for users to tag actions so that corresponding results can then be highlighted in reporting.		
55		3.1.j	The platform should provide a MITRE ATT&CK Dashboard and a Heatmap, Dashboard that highlight the areas of concern that should be prioritised by BANK SoC Team	Platform provide's MITRE ATT&ck framework dashboard to choose the attacks from	Please be guided as per RFP.
56		3.1.k	The Platform should provide information and guidance on remediation of identified results. The platform should provide ample information on the specifics of each attack in order to enable BANK SoC Team and different other Teams (Network, Endpoint, Email, DataCenter, CBS etc.) to remediate any issues encountered.	This is provided by the consulting team, the platform will not automatically provide this.	Please be guided as per RFP.

57		3.1.l	The Platform should support safe running of advanced/malicious testing in production environment against security controls within a confined isolated virtualization environment for the testing of endpoint security controls against destructive behaviors such as destructive malwares and ransomwares. This will include a BANK's Golden Image (which is rolled back to normal condition after each test). All traffic is blocked except 443 to the repository containing the IoCs (Indicators of Compromise) only.	The platform performs safe emulations, however it is recommended that this exercise be done in a staging/sandbox environment.	Bidder has to provision the same.
58		3.1.n	The platform should support executing external attacks from internet towards internal controls	This is done by the consulting team with the help of the tools.	Please be guided as per RFP.

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
59	NA	General Query	General Query	Please clarify if any changes / configurational updates are required to carry out the activities as per the scope of work within the PNB network, will be handled by PNB team or the bidder.	Please be guided as per RFP.
60	9	3. SCOPE OF WORK:	For On-Premise based Red Team capability solution; The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs	Please clarify if the bidder is required to propose and deploy a single solution or multiple integrated solutions to fulfil the requirements as per scope of work (Section 3)	Please be guided as per RFP.

61	11	3. SCOPE OF WORK: 3.4 Social Engineering	a) Vendor and Bank are required to determine a target list of Bank's employees and the scenarios used for social engineering.	Please suggest how many bank employees will be targetted for the activity, additionally, will the scenarios be different with respect to the designation of the employee or other criteria.	All Employees. However, each exercise will be limited to 10,000 employees.
62	12	3. SCOPE OF WORK: 3.4 Social Engineering	h) The solution should have support of more than 15 languages for creating phishing scenarios	Please clarify what all 15 languages needs to be incorporated into the tool, this will help us in creating the customized scenario as per requirement.	Please be guided as per RFP.
63	26	ANNEXURE I : Terms and Conditions	11. Penalty	KPMG shall not be liable for Penalty in this clause if default/delay/error/variation is not solely on account of KPMG	Please be guided as per RFP.
64	30	ANNEXURE I : Terms and Conditions	IP Infringement indemnity	We request you to bring this within the liability cap	Please be guided as per RFP.
65	30	ANNEXURE I : Terms and Conditions	30. LIMITATION OF LIABILITY	We request you to restrict our liability arising from IP infringement indemnity to a maximum of the contract value.	Please be guided as per RFP.
66	6	GENERAL TENDER DETAILS	Last date and time for Online Bid Submission/Hash submission	We request you to extend bid submission for 2 weeks i.e 25.01.2021	Please be guided as per RFP.
67	32	ANNEXURE-III : ELIGIBILITY CRITERIA OF THE BIDDER	The bidder should be registered with Registrar of Companies/Firms in India for at least 5 years.	Request you to amend this clause as: The bidder must be incorporated and registered in India under the Indian Companies Act 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or as amended or Indian Partnership Act 1932 and should have been in operation in India at least 5 years.	Please be guided as per RFP.

68	32	ANNEXURE-III : ELIGIBILITY CRITERIA OF THE BIDDER	Banks existing vendors who are auditors, security Integrators, Network integrators as on bid submission date will not be allowed to participate in this RFP.	Request to please amend this criteria as it will be an independent assessment exercise that shall be performed by teams with different skill set.	Please refer to Corrigendum-1, Sr no -1
----	----	--	--	---	---

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
69	11	Clause Name:- For On-Premise based Red Team capability solution Clause No:- 3.1 point number "h"	The platform should support integration with vulnerability management and it should also be able to detect the vulnerabilities which can be exploited.	Requesting to delete this clause as it is not relevant to the Red Team capability and should be in the scope Vulnerability Assesments which is not the scope of this RFP.	Please be guided as per RFP.
70	11	Clause Name:- For On-Premise based Red Team capability solution Clause No:- 3.1 point number "i"	The Platform should support several integrations out of the box, namely to SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, and furthermore also provides an open API that vulnerability management platforms can connect to either directly or via an orchestration and automation platform. The platform should support vulnerability prioritization based on simulation score. The platform shouldn't just test endpoint security controls, it also should test the performance of network security controls (like firewalls, proxies, IDS/IPS). This means that test results need to be interpreted in context. As an example, maybe a server has an identified	Requesting to read this clause as below The Platform should support several integrations out of the box, namely to SIEM, SOAR, WAF, Proxy, Deception, Mail gateway, IDS/IPS, firewall and other security devices/solutions and endpoints and threat intelligence platforms, and furthermore also provides an open API that vulnerability management platforms can connect to either directly or via an orchestration and automation platform. The platform shouldn't just test endpoint security controls, it also should test the performance of network security controls (like firewalls, proxies,	Please be guided as per RFP.

			vulnerability, but tests should show that either (or both) the endpoint and the firewall actively detect and block the corresponding exploit. This could significantly lower the criticality of the vulnerability. As a result, the platform provides the ability for users to tag actions so that corresponding results can then be highlighted in reporting.	IDS/IPS). This means that test results need to be interpreted in context. As an example, maybe a server has an identified vulnerability, but tests should show that either (or both) the endpoint and the firewall actively detect and block the corresponding exploit. This could significantly lower the criticality of the vulnerability. As a result, the platform provides the ability for users to tag actions so that corresponding results can then be highlighted in reporting.	
--	--	--	--	--	--

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
71	35	ANNEXURE-III ELIGIBILITY CRITERIA OF THE BIDDER; Clause No-2	Banks existing vendors who are auditors, security Integrators, Network integrators as on bid submission date will not be allowed to participate in this RFP.	This clause will restrict the bidders from participation, to maximize the bid participation and for a healthy competition we request you to kindly delete this clause	Please refer to Corrigendum-1, Sr no -1
72	35	ANNEXURE-III ELIGIBILITY CRITERIA OF THE BIDDER; Clause No-3	Bidder should be preferably CERT-IN empaneled vendor as on date of bid submission of this RFP. The clause is optional.	In order to maximize the bid participation and for a healthy competition we request you to kindly delete this clause.	Please be guided as per RFP.
73	35	ANNEXURE-III ELIGIBILITY CRITERIA OF THE BIDDER; Clause No-7	Bidder should have experience in Red Team Exercise assignment completed in at least 01 BFSI sector.	We request the bank to kindly amend this clause as: Bidder/OEM should have experience in Red Team Exercise assignment completed in at least 01 BFSI sector/ Govt. Organization/ PSU/ Private Organization in India.	Please refer to Corrigendum-1, Sr no -2

74	36	ANNEXURE-III ELIGIBILITY CRITERIA OF THE BIDDER; Clause No-8	The Bidder should have at least 05 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ any other Red Team or Penetration Testing related certification as full time employee.	We request the bank to kindly amend this clause as: The Bidder should have at least 05 Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC- Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ any other Red Team or Penetration Testing related certification as full time employee.	Please be guided as per RFP.
75	27	Annexure-I;TERMS AND CONDITIONS; Clause No-9	The invoices shall be raised after completing the whole round of Red Team Exercise as per scope of work mentioned in the RFP and payment shall be released within 30 days from the receipt of undisputed invoices by bank. In case of any dispute regarding the invoice will be communicated to the selected bidder within 15 working days from the date of receipt of the invoice.	We request you to kindly make the payment of platform on supply and payment of Red Team Exercise quarterly in advance	Please be guided as per RFP.

S.No	RFP Pg No	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Banks Reply
76	9	3.1 (a to o)	The Bidder should also propose and deploy an On-Premise automated tool for PNB Staffs to perform below activities.	<p>Cisco Red Team does not require any automated platform to be deployed in customer premises to conduct the assessment.</p> <p>If a tool is still required by PNB as asked in the RFP, please clarify details of any similar commercial tool / platform complying with the specifications as asked.</p>	Please be guided as per RFP.
77	13	3.5 l	From the samples provided, the bidder should be able to differentiate genuine and suspected fraudulent behavior.	Please clarify what does 'samples' mean?	Please be guided as per RFP.
78	13	3.5 o	In case of each simulation, there should be feature for rollback wherever required.	Please clarify what does 'roll back' mean, with a few examples.	Please be guided as per RFP.
79	13	3.5	Red Team Assessment	Cisco conducts Red Team assessments in a comprehensive method. Each scenario roughly takes around 25 to 30 days including report. Internal Assume Breach Red Team scenarios would require (but not limited to) a testing setup, and remote VPN access into the network. Kindly clarify if these logistics can be provided to the Cisco team.	Please be guided as per RFP.
80	12	3.4 d to l	Social Engineering	There is a mention of a solution and its capabilities. Please clarify that all requirements as given in the RFP are to be accomplished by the Vendor and no single commercial tool / solution is required to be demonstrated.	Please be guided as per RFP.

81	11	3.3	Training: Vendor is required to impart training to the identified bank personnel/ SOC team on the platform, functionality and services	Please clarify details of training required and on which Platform. Cisco conducts a debrief on the Red team assessment and its success in the Bank's environment to the Blue team so that lessons can be drawn to strengthen the security framework.	Please be guided as per RFP.
82	25	6	EXECUTION OF ORDER	We would request Bank to allow 6 weeks from Date of acceptance of letter of Offer.	Please be guided as per RFP.
83	25	7	RED TEAM EXERCISE TIME	We would request Bank to allow 2 weeks within completion of Red team exercise	Please be guided as per RFP.
84	25	9	Payment	We would request Bank to consider Standard Quarterly Advance Payment so that bidder will able to structure the deal financing.	Please be guided as per RFP.
85	26	11	Penalty	Request if Bank can cap the maximum penalty to 5% overall Contract Value	Please be guided as per RFP.
86			OEM Services	We would request Bank to allow Bidder to quote OEM Red Team Services	Please be guided as per RFP.
87	35	3	Bidder should be preferably CERT-IN empaneled vendor as on date of bid submission of this RFP. The clause is optional.	We would request Bank to remove this clause so that OEM can bid through their resellers	Please be guided as per RFP.
88	35	7	Bidder should have experience in Red Team Exercise assignment completed in at least 01 BFSI sector.	We would request Bank to remove this clause so that OEM can bid through their resellers	Please refer to Corrigendum-1, Sr no -2

89	36	8	The Bidder should have at least 05 Offensive Security Certified Professional (OSCP) from offensive-security/ Certified Ethical Hacker (CEH) from EC-Council/ Licensed Penetration Tester (LPT) from EC-Council / GPEN: GIAC Penetration Tester from SANS/ GWAPT: GIAC Web Application Penetration Tester from SANS/ any other Red Team or Penetration Testing related certification as full time employee.	We would request Bank to consider Bidder / OEM for this clause.	Please be guided as per RFP.
----	----	---	--	---	------------------------------