REQUEST FOR PROPOSAL FOR PROCUREMENT OF SOFTWARE SOLUTION/ SERVICE OF BREACH AND ATTACK SIMULATION SOLUTION

Ref: SBI/GITC/ISD/2023-24/SOC/15 dated: 22/09/2023

Bank's response/clarifications to the queries by the bidders

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
1	55	D4	Proposed solution must have the ability to validate data loss prevention (DLP) implementation, methodology, and configuration and customization along with other exfiltration techniques like USB, cloud service, email, etc and protocols to test outbound data flow	are we supposed to cover following methods of exfiltration as well namely HTTP, HTTPS, DNS, DNS tunnelling, SFTP, open ports, cloud services, email, Gmail, browser HTTP, browser HTTPS.	Proposed solution should be attack method agnostics. Also, it should support customization of all probable attack to validate data exfiltration.
2	56	D-9	The solution should have capabilities to instrument simulation on following: 1. End-Points 2. Web Gateway 3. Web Application Firewall (WAF) 4. Proxy 5. Email Based Attacks 6. Advanced Persistent Threat (APT) 7. Any combination of above lists	Email attack: are we supposed to cover methods like links, sandbox testing, forged extensions?	Proposed solution should ensure all possible attack methods and techniques. Due to the dynamic nature of attack a static template is not recommended to use for attack simulation as the Tactics, Techniques, and Procedures (TTPs) of the attackers keep evolving by the time. It is imperative to have all possible TTPs.
3		D-9		WAF Attack: details of what type of WAF bypass techniques needs elaboration namely SQL injection, XSS, file inclusion…	
4	58	D-21	Proposed solution should have the feature of cyber risk quantification.	Proposed solution should have the feature of cyber risk quantification. … Kindly elaborate. Quantifying cyber risk based on internal misconfigurations Or from external attack surface perspective Or combined?	The proposed solution should provide risk quantification which is not limited to internal or external attack simulation. However, it should be on the basis of individual simulation technique and over all attack simulation separately to

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
					evaluate risk exposure and its impact over the period of time. Hence, the bidder should comply with the clause.
5	52	A-3	The simulation agent / sensor should be compatible on Windows, Non- Windows (All flavours including but not limited to Ubuntu, RHEL, Cent OS), Apple's MAC OS etc.	The simulation agent / sensor should be compatible on Windows, Non-Windows (All flavours including but not limited to Ubuntu, RHEL, Cent OS) etc.	Mac OS is available in Bank's environment. Hence, the requirement shall be remained same.
6	53	B-3	Proposed solution supplier shall provide the assurance and evidence that no PII and SPII (sensitive personally identifiable information) data is being transmitted from the Bank's environment to OEM's cloud instance.	Need More Information	Proposed solution in case of on premise wherein threat DB update via push in or SaaS based, or any attack simulation like lateral movement wherein the host traversal information may captioned should not go outside the Bank's boundaries. This has addressed in pre-bid meeting.
7	55	C-2	The solution must be directly integrate and compatible with common commercial endpoint security controls like Antivirus (AV), End-Point Detection & Response (EDR), and Data loss prevention (DLP) etc.	Request to share list of security solutions (AV/EDR/DLP etc.)	The proposed solution should be Antivirus (AV), End-Point Detection & Response (EDR), and Data loss prevention (DLP) agnostic.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
8	55	C-4	The solution must include support of Advance authentication / MFA for Email access.	Need More Information	The proposed solution should be Email provider agnostic and support MFA (Multi factor authentication).
9	57	D-15	Proposed solution should have the ability to simulate the lateral movement across endpoints, specific IPs, subnet and target AD group etc.	Request to relax / remove this clause	Bidder must comply with the requirement.
10	58	D-18	Proposed solution should have the ability to identify the device trajectory to map how host interact with files across end-points	Need More Information	This is the case of lateral movement, the proposed solution should provide graphical view to highlight all accessed devices and the routes for accessing those devices. Further, the clause is “Preferred”.
11	59	D-28	Solution should be equipped with the continuous discovery, inventory, classification and monitoring of the external/public facing IT infrastructure and digital assets of the Bank.	Request to relax / remove this clause	Bidder must comply with the requirement.
12	59	D-31	Proposed solution must have facility to send periodic notifications summarizing changes to the Bank’s attack surface.	Request to relax / remove this clause	Requirement shall remain same. However, its “Preferred” requirement. Bidder must comply with the requirement.
13	59	D-34	Service provider must be an active collaborator with Computer Emergency Response Team (CERT) of the countries for IOC and Threat Feeds. It should uphold a defined SLA (no more than 24 Hrs) on adding new attacks identified from CERT.	Need More Information	The proposed solution must have playbook/attack template available within 24 Hrs as per the threat feeds/IOC received from various Computer Emergency Response Team

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
					(CERT). Bidder must comply with the requirement.
14	59	D-35	Service provider must be recognized by the industry experts in its market research reports published for Breach and Attack Simulation. For example Gartner's Magic Quadrant, or any internationally recognized organizations.	Request to allow Gartner Peer Insights. Request to relax / remove this clause for Make In India OEM.	It's a "Good to have" requirement.
15	50	Appendix-B-SN.7	"Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 03 BFSI client references are required). Preference will be given the PSB/PSU and other government Bodies. "	Request to change from 3 BFSI reference to 1 BFSI reference.	Bidder must comply with the requirement.
16	52	A-2	Bidder has to provide documents (SOC-2 Report, Pen Test Report, CAIQ (Consensus Assessments Initiative Questionnaire etc) pertaining to their infra audit process.	Request for more details	Please advise, what specific details is needed to comply.
17	68	Appendix-E S.N. 19	In ordered invoice should be in INR (Indian Rupees), shall be processed quarterly arrear basis.	In ordered invoice should be in INR (Indian Rupees), shall be processed quarterly ADVANCE basis.	Bidder must comply with the requirement.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
18	52	A-1	The solution must be deployable in a production on-premises/on-premises Private Cloud/India based Public cloud/ Public-Private Hybrid India based Cloud environments.	Bank wanted all deployment methods should be possible with the BAS solution or any one of mentioned in the technical specification	Please refer to Corrigendum-2 for revised clause.
19	52	A-4	The solution must support proxy communications to the internet. Simulation Agents installed must support proxy communications to the proposed solution's platform counterpart. The proposed solution should be proxy OEM agnostic.	Support for explicit or implicit proxy? Please clarify	The solution must support bank's configured proxy where in the visibility of the traffic can be monitored.
20	54	B-6	The solution must support role-based access control (RBAC) so that discrete privileged and user account with specific permissions can be created.	Any Specific kind of RBAC bank is referring to and privileges to be assigned to user? Please clarify.	The solution must support role based user creation like administrator/non-administrator.
21	54	B-9	Proposed solution does not store or transmit credentials in clear text/ unencrypted form.	Is this for management console of the tool/solution or for assessments as well? Please clarify	Any traffic initiated from/to solution/tools should not be in clear text. This covers the management console as well as any assessment performed.
22	54	B-10	The proposed solution must fulfill the compliance requirement for Data Protection & Privacy etc published by Govt. of India, Regulated Entity etc within the stipulated time.	Any specific data compliance bank is referring to?	All regulatory compliance applicable to Bank.
23	54	C-1	The solution must be SIEM vendor agnostic and it should have the capability to directly integrate with common commercial SIEM solutions available in market.	Bank is referring to pre-defined templates within the tool to integrate the SIEM?	The solution should be able to integrate with SIEM solution as per Bank's configuration.
24	55	C-3	The solution should support advanced security protocols for communication.	Please share the use case for the advance security protocols, or bank is referring to custom protocols.	The solution should not use deprecated communication protocols like SSL, TLS1.0 etc.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
25	56	D-10	The solution should have ability to integrate and consume threat feeds such as IOC, Hashes, IPs etc from RE (Regulated Entities) like CSITE, CERT-IN, RBI etc to create custom use cases simulation.	Integration of Threat Feeds to Solution through any method is considered by the Bank?	The bidder shall ensure that available threat feeds should be automatically updated in the solution.
26	57	D-14	Proposed solution should simulate the non-intrusive assessment of Bank's public facing applications. There should not be any cap for the application to be assessed.	This point is for Application security/ penetration testing as to simulate the application facing internet? Please clarify	All automated assessment which can be performed on Bank's public facing touchpoints is being referred here.
27	58	D-26	Proposed solution should support for the creation of custom use cases of attack simulation on the basis Zero Days attack / vulnerability or Global Threat feeds.	Custom use case is editing payload for each use case? Please clarify	More elaboration required on the query.
28	50	Eligibility Criteria	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 03 BFSI client references are required). Preference will be given the PSB/PSU and other government bodies.	Request that the ask be reworded to " Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder/ OEM has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 02 BFSI client references are required). Preference will be given to Banks, PSB/PSU and other government bodies." so that more bidders can participate and make the RFP competitive	Bidder must comply with the requirement.
29	67	Integration / Migration Requirements	The solution needs to support integration with the Bank's current security and operations management systems like SOC, PIMS, DLP,AD, ITAM, Proxy, etc.	Kindly specify the solution names for all existing solutions were integration is expected	The requested information shall be shared only with the qualified bidder.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
		with existing systems			
30	50	Bidder's Eligibility Criteria	The bidder, if participating as Channel Partner of any OEM, then OEM should have a support center and level 3 escalation (highest) located in India.For OEMs, directly participating, the conditions mentioned above for support center remain applicable.	Request that the ask be reworded to "The bidder on award of the project as Channel Partner of any OEM, then OEM should provide for a support center and level 3 escalation (highest) located in India. For OEMs, directly participating, the conditions mentioned above for support center remain applicable." this will ensure that more bidders can come in with a commitment to provide same level of support.	Bidder must comply with the requirement.
31	83	Appendix M	Appendix asks for Value of Work Order (In Lakh) (only single work order)	The Value of Work Order may not be shareable because of various NDA clauses with the customers and should be removed from the Appendix M	Please refer to Corrigendum-2 for revised clause.
32	53	Technical & Functional Specifications B-Compliance and Security Aspects	The cloud instance must be in India region only and dedicated to the SBI.	Please make it optional as this is required only in case offering is cloud based. In case where service provider gives complete on-prem solution this becomes not Applicable.	Please refer to Corrigendum-2 for revised clause.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
33	58	Functional and Technical Requirement	The solution should supports prominent cloud OEMs or the hosted application like Azure, AWS, Google Cloud etc.	IS bank looking for cloud security posture management Solution or looking to validate security controls deployed in could using BAS threat repository	Yes, bank may use the BAS solution for validating the security controls of the hosts provisioned in cloud environment.
34	59	Functional and Technical Requirement	The solution should have the ability to run social engineering attacks	We request you to consider this point as Social engineering attack involves human intervention to click on a ink etc and Bas solution deals with real worked pay loads and it will be dangerous to send mails to the user. This solution van better addressed by phishing solutions and pen tester. This is a pen test approach. Partner can offer this.	Bidder must comply with the requirement.
35	60	Executive Reporting & Dashboards	Executive dashboard and reports should be available in the solution which can be customized as per Bank's requirement.	Solution must support APIs for generating customized dashboards. And service provider should be able to provide the same with no additional cost to the Bank.	Please refer Corrigendum-2 for revised clause.
36	61	Executive Reporting & Dashboards	Report encryption based on customized key should be available in the solution	Many vendors don't support customized keys for encryption. Please change the clause to The solution must store the report in encrypted form. In there a solution with industry-standard like AES-256	Report encryption based on user supplied password should be available in the solution.
37	9	4i	Service Provider shall ensure that the remote access to the Bank's VPN is performed through a laptop/desktop ("Device") specially allotted for that purpose by the Service Provider and not through any other private or public Device.	IS SBI VPN going to be used	Bidder must comply with the VPN requirement of the Bank.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
38	9	4ii	Service Provider shall ensure that only its authorized employees/representatives access the Device. iii. Service Provider shall be required to get the Device hardened/configured as per the Bank's prevailing standards and policy.	Is the customer SOE going to be followed? How Laptop is going to hardened and what is the Banks policy which is going to be followed for device (Laptop/desktop) hardening and configuration	The requested information shall be shared with qualified bidder. As the requested information is sensitive in nature.
39	9	4iv	Service Provider and/or its employee/representative shall be required to furnish an undertaking and/or information security declaration on the Bank's prescribed format before such remote access is provided by the Bank.	Does SBI provide undertaking - If yes, then this can be monitored through RIGHTs.	Service Provider and/or its employee/representative shall be required to furnish an undertaking provided by the Bank.
40	9	4v	Service Provider shall ensure that services are performed in a physically protected and secure environment which ensures confidentiality and integrity of the Bank's data and artefacts, including but not limited to information (on customer, account, transactions, users, usage, staff, etc.), architecture (information, data, network, application, security, etc.), programming codes, access configurations, parameter settings, executable files, etc., which the Bank representative may inspect. Service Provider shall facilitate and/ or handover the Device to the Bank or its authorized representative for investigation and/or forensic audit.	Only relevant if N/W components or infra is dedicated for customer, not applicable for shared infra.	Bidder must comply with the requirement. Since deployment shall be done on dedicated infrastructure for this project.
41	9	4vi	Service Provider shall be responsible for protecting its network and subnetworks, from which remote access to the Bank's network is performed, effectively against unauthorized access, malware, malicious code and other threats in order to ensure the Bank's information	How is the connectivity going to be establied? Any dedicated link, N/W components etc. Accordingly this point need to be looked at.	In case of on-perm infrastructure, no remote access shall be granted from outside the Bank. However, for SaaS based solution bidder should comply Bank's policy.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
			technology system is not compromised in the course of using remote access facility		
42	22	25	System integration testing will be followed by user acceptance testing, plan for which has to be submitted by Service Provider to the Bank. The UAT includes functional tests, resilience tests, benchmark comparisons, operational tests, load tests etc. SBI staff / third Party vendor designated by the Bank will carry out the functional testing. This staff / third party vendor will need necessary on-site training for the purpose and should be provided by Service Provider. Service Provider should carry out other testing like resiliency/benchmarking/load etc. Service Provider should submit result log for all testing to the Bank.	Is UAT going to be done from customer environment	Yes
43	23	25	Service provider will also ensure the successful completion of Security Review conducted by Bank's information security department. After successful security review limited trial period shall be start.	what does it mean by limited trial period to start.	Please refer Appendix-E S.No. 15
44	23	26vi	Bidder shall inform and implement patches/ upgrades/ updates for hardware/ software/ Operating System / Middleware etc as and when released by Service Provider/ OEM or as per requirements of the Bank free of cost.	If customer SOE will be deployed on Bidder assets, then bidder will not be responsible for any kind of updates on systems. Also, need clarity whether the Infra will be managed by bidder.	Please elaborate your query in context of infrastructure.
45	23	26vii	Bidder shall obtain a written permission from the Bank before applying any of the patches/ upgrades/ updates. Bidder has to support older versions of the hardware/ software/ Operating	If customer SOE will be deployed on Bidder assets, then Bidder will not be responsible for any kind of updates on systems. Also, need clarity whether the Infra will be managed by bidder.	Please elaborate your query in context of infrastructure.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
			System /Middleware etc in case the Bank chooses not to upgrade to latest version.		
46	23	26viii	Bidder shall provide maintenance support for Hardware/ Software/ Operating System/ Middleware over the entire period of contract.	Does the Infra need to be maintained by bidder.	All infrastructure for this project shall be managed by the Bidder/OEM.
47	25	27vi	In the event of system break down or failures at any stage, protection available, which would include the following, shall be specified. (a) Diagnostics for identification of systems failures (b) Protection of data/ Configuration (c) Recovery/ restart facility (d) Backup of system software/ Configuration	Which Back up policy will be followed. What tool will be used for backup, data recovery and identification of systems failures.	Back-up shall be done as per Bank's policy. Further, back-up frequency, type etc. shall be defined in SLA.
48	26	30a	Service Provider shall intimate the Bank before dispatching products for conducting inspection and testing	Testing done by whom and is it in scope of Bidder.	Please refer section 30 point 1 of the RFP.
49	26	30b	The inspection and acceptance test may also be conducted at the point of delivery and / or at the products' final destination. Reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors, at no charge to the Bank. In case of failure by Service Provider to provide necessary facility / equipment at its premises, all the cost of such inspection like travel, boarding, lodging & other incidental expenses of the Bank's representatives to be borne by Service Provider	Right to audit clause must be agreed in the MSA/contract and Bidder's NDA to be signed by the auditor before the visiting to the factory site of the service provider for inspection. Does the delivery takes place from Bidder premises or customer location	This project shall not be part of MSA. Bidder may provide the NDA to be signed by the auditor before the visiting their site.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
50	26	30v	System integration testing and User Acceptance testing will be carried out as per requirement of the Bank.	Is testing in Scope of Bidder.	No, Bank shall perform test and Bidder/OEM shall provide the comprehensive walkthrough to identify Bank's officials.
51	26& 27	31i	The Selected Bidder (Service Provider) shall be subject to annual audit by internal/ external Auditors appointed by the Bank/ inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/ such auditors in the areas of products (IT hardware/ Software) and services etc. provided to the Bank and Service Provider is required to submit such certification by such Auditors to the Bank. Service Provider and or his / their outsourced agents / sub – contractors (if allowed by the Bank) shall facilitate the same The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Except for the audit done by Reserve Bank of India or any statutory/regulatory authority, the Bank shall provide reasonable notice not less than 7 (seven) days to Service Provider before such audit and same shall be conducted during normal business hours	As per the scope of this engagement. This needs to be agreed as per contract.	Bidder must comply with the requirement

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
52	30& 31	39	INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP:	IPR will be with Bidder or customer?	Bidder must comply with the requirement
53	43	55ii	In continuation to above details, Non-Disclosure Agreement (NDA) which needs to be signed by the bidder and each OEM and their onsite resources individually and visiting officials.	Is it SBI NDA to be signed with OEM	Yes
54	50	Appendix B 8	SOC-2 and ISO-27001 standard Valid Certificate(s) to be provided mandatorily.	Bidder is certified for ISO 27001. SOC is done as per project requirement	SOC-2 report is a mandatory report requirement which needs to be shared with the Bid document.
55	52	Appendix C A-1	The solution must be deployable in a production on-premises/on-premises Private Cloud/India based Public cloud/ Public-Private Hybrid India based Cloud environments.	Delivery to understand whether it is going to be on-prem or cloud (whether public, private)	The solution must be deployable in any one of the following method On-premises/on-premises Private Cloud/India based Public cloud/ Public-Private Hybrid India based Cloud environments. However all infrastructure cost shall be borne by the bidder.
56	3		EMD amount to be deposited in A/c No: 4897932113433	It is requested to change this clause as EMD to be in the form of NEFT/ RTGS or equivalent amount of BG to be submitted with validity period of 180 days.	Bidder must comply with the requirement
57	11		The EMD should be directly credited to the designated account as mentioned in Schedule of Events. Proof of remittance of EMD in the designated account should be enclosed with the technical bid.	It is requested to amend this clause. There should be option to deposit EMD in the form of BG for validity period of 180 days.	Bidder must comply with the requirement

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
58	31 & 32	40	LIQUIDATED DAMAGES: If the Service Provider fails to deliver product and/or perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 10% of total Project Cost.	It is requested to amend this clause as LIQUIDATED DAMAGES: If the Service Provider fails to deliver product and/or perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost.	Bidder must comply with the requirement
59	64-68	Appendix-E	Contract Period: 2 Years, Post successful installation and Go live Phase.	It is requested to change the payment term. Cost of the third-party HW & SW should be paid upfront on delivery of those HW & SW. Other charges may be paid on quarterly basis.	Bidder must comply with the requirement
60	74	Appendix-I	All penalty amount will be calculated on the total amount of project cost annually. The maximum penalty that can be claimed will be 10% of the project cost.	It is requested to amend this clause. All penalty amount will be calculated on the total amount of project cost annually. The maximum penalty that can be claimed will be 5% of the project cost.	Bidder must comply with the requirement
61	58	D-26	Proposed solution should support for the creation of custom use cases of attack simulation on the basis Zero Days attack / vulnerability or Global Threat feeds.	Bidder requested the clarification in pre-bid meeting	Proposed solution must have the feature for creation of use cases to validate the bypass/penetration/exfiltration in Bank's IT- eco-system.

#	Page	RFP Ref	Existing Clause	Bidder Query	Clarification
62	85	D-5	The solution must be able to report vulnerability/security gaps risk severity (Critical, High, Medium, Low and Informative) based on proven cybersecurity risk assessment Models / framework. (e.g: DREAD, CVSS, NIST etc)	Bidder requested the clarification in pre-bid meeting.	Penetrated/ Exfiltrated /By-passed simulated method should have classified on the basis of risk severity defined globally accepted risk assessment framework.