केनरा बैंक Canara Bank

Corrigendum-2 to GeM Bid ref: GEM/2022/B/2885701 dated 27/12/2022 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach and Attack Simulation Solution in Canara Bank for 3 years

It is decided to amend the following in respect of the above GeM bid:

a. GeM Bid Document, Bid Details (Bid End Date/Time, Bid Opening Date/Time, Page no. 1 of 6):

Description	Existing details	Amended details
Bid End Date/Time	24-01-2023, 17:00:00	30-01-2023, 17:00:00
Bid opening Date/Time	24-01-2023, 17:30:00	30-01-2023, 17:30:00

Sl. No.	Section/ Annexure/ Appendix of the GeM bid	Clause No.	Existing	Amended
b.	Additional Terms and Conditions (ATC)	17. Escrow arrangement	Existing clause	This clause stands deleted.
c.	Additional Terms and Conditions (ATC)	20. Payment terms	Existing clause	The amended Payment terms is attached to this corrigendum as Annexure-A.
d.	Additional Terms and Conditions (ATC)	Annexure-2 Technical and Functional Requirements	Existing clause	The amended Annexure-2 is attached to this corrigendum.
e.	Additional Terms and Conditions (ATC)	Annexure-11 Technical Evaluation Criteria	Existing clause	The amended Annexure-11 is attached to this corrigendum.

All the other instructions and terms & conditions of the above GeM bid shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject GeM bid.

Date: 20/01/2023
Place: Bengaluru

Deputy General Manager

D.I.T. Wing, Procurement Group CANARA BANK HO, Bengaluru-560001

Amended Annexure-11

1. Payment terms:

1.1. The payment schedule will be as under and will released after execution of contract agreement:

Sl. No.	Description of Items and services	Reference in Annexure-12 i.e. Bill of Material	Payment terms
a.	Hardware/Appliance including OS for DC & DRC Locations.	Line item no. 1, 2, 3 & 4 of Table-A of Annexure-12	➢ 40 % of the payment will be released on delivery as per clause 12 of the ATC document. ➢ 50 % of the payment will be released on full implementation and sign-off from the Bank as per clause 12 the ATC document. ➢ 10 % of the payment will be released: After completion of warranty period and after deducting applicable penalties and Liquidated damages. Or On submission of a bank guarantee for equivalent to 10% of the remaining payment.
b.	System Software/ Middleware/ Database License for deploying proposed Solution at DC & DRC Locations.		
c.	Any Other Software licenses.		
d.	One Time Implementation charges	Line item no. 5 of Table-A of Annexure-12	100% payment will be released on full implementation and sign-off from the Bank as per clause 12.4. the ATC document.
e.	Licenses for Breach and Attack Simulation Solution as per Annexure-1 & Annexure-2	Line item no. 1 of Table-B of Annexure-12	➢ 50 % of the payment will be released on delivery as per clause 12 the ATC document. ➢ 40 % of the payment will be released on full implementation and sign-off from the Bank as per clause 12 of this document and Completion of training and performing at least 5 assessments.

			➢ 10 % of the payment will be released: After completion of warranty period and after deducting applicable penalties and Liquidated damages. Or On submission of a bank guarantee for equivalent to 10% of the remaining payment.

1.2. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.

1.3. Bank will release the payment on completion of activity and on production of relevant documents/invoices. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's / Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.

1.4. The selected bidder has to submit installation report/Sign off report duly signed by the Bank officials of the respective Branch/offices in originals while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.

1.5. Bank will not pay any amount in advance.

1.6. Payment shall be released within 30 days from the date of submission of relevant documents as per GeM bid terms and found in order as per GeM bid terms..

1.7. The bank shall finalize the installation and acceptance format mutually agreed by the selected bidder. The selected bidder shall strictly follow the mutually agreed format and submit the same for each location wise while claiming installation and acceptance payment.

1.8. The payments will be released through NEFT / RTGS after deducting the application LD/Penalty, TDS if any, by centrally by Head Office at Bengaluru and the selected bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code etc.

केनरा बैंक Canara Bank

Amended Annexure-2

Technical and Functional Requirements
(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach and Attack Simulation Solution in Canara Bank for 3 years.

Ref: GeM Bid: GEM/2022/B/2885701 dated 27/12/2022.

Note:	
(a)	If the bidder feels that certain features offered are superior to what has been specified by the Bank, it shall be highlighted separately. Information regarding any modification required in the proposed solution to meet the intent of the specifications and state-of-the-art technology shall be provided. However, the Bank reserves the right to adopt the modifications /superior features suggested/ offered.
(b)	The bidder shall provide all other required equipment's and/or services, whether or not explicitly mentioned in this GeM bid, to ensure the intent of specification, completeness, operability, maintainability and upgradability.
(c)	The selected bidder shall own the responsibility to demonstrate that the services offered are as per the specification/performance stipulated in this GeM bid and as committed by the bidder either at site or in bidder's work site without any extra cost to the Bank.

A. TECHNICAL REQUIREMENTS

Sl. No.	TECHNICAL REQUIREMENTS	Mandatory	Bidder's Compliance (YES/NO)	Remarks
1.	INFRASTRUCTURE			
1.1.	Bidder to provide details of the infrastructure, hardware, software, power supply, storage and connectivity details.	Yes		
1.2.	Bidder to provide the technical escalation matrix	Yes		
1.3.	Bidder to provide documents pertaining to the audit process being followed by them.	Yes		
1.4.	The selected Bidder shall guarantee a Monthly uptime of minimum 98.0% for the Backend Infrastructure (hardware/software from the date of commencement of the proposed solution. (Any planned shutdown will not be considered for calculating SLA).	Yes		
2.	ACCESS CONTROL			
2.1.	Access to the System by Bank as well as proposed Vendors should be by way of User-Id & Password and should support	Yes		

	the banks current policy & systems for Access control and should be able to integrate seamless with any IDAM (Identity and Access Management) solution procured in future.			
2.2.	The system should have at least 2 levels of Access Control at Bank: a. Administrator - who will be the Super User and create Internal Users b. Users - Users who use the system for proposed functionalities	Yes		
3.	OTHER REQUIREMENTS			
3.1.	Bidder to provide details of implementation team along with appropriate experience in similar projects.	Yes		
3.2.	The solution must have the capability to simulate inside-out and outside-in attack.	Yes		
4.	SYSTEM SUPPORT			
4.1.	The offered solution should have support for the following client side features: 1. Operating Systems: Windows 7, Windows 8, Windows 10 and above. 2. Internet Browsers: a) IE 9, 10, 11 and above. b) Google Chrome Version 51 and above.	Yes		

B. FUNCTIONAL REQUIREMENTS

Sl.no.	Functional Requirement	Marks
1	All installed agents/simulators, if required, should have capability to run assessments/simulations as local user privilege or admin user privilege.	1
2	The simulation agent should be compatible on various platforms like Window, Linux, MAC OS etc.	1
3	The solution should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations.	1
4	The agent installed for assessments /simulations should be able to remove any malicious files or executables that were run on the system as part of the simulation activity.	1
5	The proposed solution should be able to provide the entire attack kill chain in accordance to MITRE attack framework. In case of change in MITRE attack framework, the tool has to adopt the revised / changed framework.	1
6	The solution should Identify controls specific effectiveness of models (MITRE, NIST) etc.	1

7	The solution should be able to determine during an attack which security solutions were able to detect the attack and if they were not able to detect then should be able to suggest rules / configurations to be done on the security solutions.	1
8	The solution should support user management with support for different user roles like admin, user etc.	1
9	The solution should be able to source latest threats in the industry and should be able to provide simulations immediately, not later than 1 day of discovery of any new threat.	1
10	The solution should be able to check any outbound flows of data / critical information, outlined by bank, during simulation.	1
11	The solution should be able to simulate Infiltration techniques for breaching a network or infecting a host.	1
12	The solution should be able to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	1
13	The solution should be able to simulate Real attacks and provide malware artefacts (capability to simulate real exploits and latest malware	1
14	The solution should be able to test attacker lateral movement (once successfully within a network) - e.g., pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data	1
15	The solution should be able to perform simulation using latest Ransomware malware samples/cases, etc.	1
16	The solution should be able to do Email security assessment (improper configuration or implementation of email filters)	1
17	Endpoint Assessment - test security state of endpoints by comprehensively testing regardless of the method used to do the assessment.	1
18	The solution should be able to perform privilege escalation during endpoint assessment.	1
19	The solution should be able to simulate access, connection or data transfer attempt while performing Network segmentation test.	1
20	The solution should be able to detect data transfer to and from malicious domains / IPs / websites (Secure web gateway / proxy test)	1
21	The solution should be able to detect the effectiveness of security tools deployed in the bank.	1
22	The solution should be able to detect the outbound exposure to malicious or compromised websites from the bank's endpoints and servers, etc.	1
23	The solution should be able to deliver safe simulations without any interference with the existing setup and chance of spreading any malware / infected files to other systems should be restricted.	1
24	The solution should have the ability to identify the device trajectory to map how hosts interact with files, including malware, across endpoint environment (eg., if the file transfer was blocked or if the file was quarantined by antivirus & security solution deployed in bank.	1

25	The solution should be able to perform continuous analysis and there should not be cap on the number of times simulations are being performed for a particular device/devices.	1
26	The solution should be able to generate detailed report covering the attacks which were successful and should detail the indicators of compromise (IoCs) and how the attack played out in the environment.	1
27	The solution should have the capability to provide the Indication of Attack (IoA) based on the tool intelligence of detecting IOCs, behavior, other contextual information etc. about the attacks.	1
28	The report generated from the solution should also provide mitigation steps that can be taken to lower the overall security risk highlighted by the simulations.	1
29	The tool should be able to customize the risk categorization. The report generated should highlight the attacks detected along with the category of the same and risk associated with them.	1
30	Determine which controls are most and least valuable; i.e., prioritization of controls.	1
31	The solution should be capable of importing data from various sources like CMDB to do prioritization.	1
32	Continuously simulate breach methods to address changing risks, and track security posture via risk trending and historical reports.	1
33	Solution should integrate with the Security Operations Centre tools and judge the effectiveness of the same by simulating multi-vector attack.	1
34	The solution should support red team activities (attack scenarios) and blue team activities (actionable remediation)	1
35	The solution should be able to create custom use cases/ simulations based on new attacks or bank's requirements.	1
36	The solution should provide an interactive user dashboard for administration and should provide the capability to the user to run only specific simulations on a set of devices.	1
37	The dashboard should display the history of previous simulations carried out and should have capacity to store historical reports for previous simulations.	1
38	The content library of the solution should be updated periodically with new attack simulations.	1
39	All the simulations should be mapped to MITRE, NIST attack framework.	1
40	The solution should not be dependent on other solutions for sourcing threat feeds.	1
41	The solution should be able to integrate with ticketing platforms.	1
42	Measure the time to detect and respond the attack simulation.	1
43	Solution should provide comprehensive report for improving configurations to target and eliminate specific weaknesses.	1

D.I.T. Wing, Procurement Group CANARA BANK H.O. Bengaluru-560001

44	The solution should have the capability of providing evidence of execution or triggering of SIEM correlation rules based on detection, blocking, alerting and/or other notification of malicious behaviour or attack.	1
45	The solution should have the capability of providing attack blocking / prevention analysis.	1
46	The solution should have the capability to execute attack sequences to expose changes in effectiveness or identify risks.	1
47	The solution should have the capability to integrate and consume threat feeds such as IOCs, IPs etc. from third party intelligence/regulators like CSITE, CERT-IN, etc.	1
48	The solution should provide RESTful API interface from third party.	1
49	The solution should not add/create any performance degradation in the network.	1
50	The solution should have the capability to instrument attacks on each of the below vectors: · Endpoint based attacks · Network based attacks · Email based attacks · Proxy · Attacks on cloud infrastructure · Any combination of the above The list is illustrative, not exhaustive. This is a mandatory requirement.	1
51	The solution should have the ability to execute complete attack library across network topology.	1
52	The solution should support cyber behavior models (MITRE ATT&CK, kill chain scenarios, CVE) , etc.	1
53	The solution should have the capability to Execute a custom data exfiltration action through email, pen-drive, SFTP etc. attempting to physically remove data from customer infrastructure.	1
54	The solution should have the ability to import, extract malicious content and weaponize PCAP attack files or malicious traffic.	1
55	The solution should have the capability to discover Network segmentation and communication path in the infrastructure where this solution is deployed.	1
56	The solution should have the capability to continuous validation the Network segmentation in the infrastructure where this solution is deployed.	1
57	The solution should have the capability of providing Detect, alerting analysis including SIEM Correlation rule analysis.	1
58	The solution should have the capability to validate existing deployed Data Loss Prevention/Protection controls.	1
59	The solution should have the ability to execute batch attack scenario processing across multiple vectors including Network, Endpoint, Email and cloud.	1

D.I.T. Wing, Procurement Group CANARA BANK HO, Bengaluru - 560001

60	The solution should be able to perform attack by exploiting the missing patches on the system & report has to be generated highlighting issues due to missing latest patches.	1
61	The solution should have the facility to integrate with the existing VA Tool of the bank to obtain information about existing vulnerabilities.	1
62	Solution should be able to validate end-point security tool controls.	1
63	Canara Bank requires that the solution must provide executive dashboards that are tailored to enable Bank with the ability to communicate effectiveness beyond the security organization to the key stakeholders.	1
64	The bidder may propose a Hybrid or on-prem deployment model and no information should be sent outside the organization, unless it has got dependency for testing any external testing component, with specific consent of the bank.	1
65	The solution should be able to import samples of sensitive data from solution such as DLP.	1
66	Ability to deliver safe tests with no chances of interfering with business operations, and no user interference when deployed on production assets	1
67	Mechanism to identify remediation options and recommendations, prioritize severity of test findings and actionable remediation for each security control.	1
68	Solution should able to do a lateral movement assessment from a single endpoint	1
69	Solution should check inbound and outbound penetration of web gateway.	1
70	All data provided by the solution or accessible on the solution by the bank should be collated from the public domain and other forums via passive scans, and other non-intrusive activities	1
71	Solution should store historical information about bank to provide cybersecurity maturity over time	1
72	Solution should make use of visual representations and dashboards to summarize and present insights and findings related to the bank	1
73	The Individuals sections of the solution should offer export of the presented data in PDF, excel and other format	1
74	Solution must include metadata and discovery artefacts associated with targets and should provide detection/discovery path(s) related to entities	1
75	Solution must illustrate changes to the attack surface of bank over time	1
76	Solution should use comprehensive technology, manual review, or other mechanisms to reduce the false positives within the dataset	1
77	The solution should provide data/ information on the bank's vulnerabilities (inherent, obsolete versions, unpatched and other types), misconfigurations, less secure configurations or unconfirmed setups, internal applications, services, URLs, ports, network components, systems, databases, and any other bank's infrastructure exposed in public domain and other forums	1

D.I.T. Wing, Procurement Group CANARA BANK HO, Bengaluru - 560029

78	The Solution should support RESTFUL API from third party	1
79	The solution shall be able to run single attacks or sequence of attacks whether pre-defined or custom and the solution must have capability to customize attack and attack plan	1
80	The solution should support customization of attack and the solution shall allow exporting data in CSV, PDF and JSON	1
81	The Solution shall support various SIEM platforms for the purposes of validating alerting and event flow into the SIEM from individual security products as well as validating proper and accurate correlated rule writing.	1

Notes:

a) Bidder should comply with each mandatory requirement and non-compliance to any of the Mandatory requirement as per Technical Specification/requirement (Annexure-2) leads to disqualification.

b) Any specification declared Compliant, however, it is found non-compliant during Technical evaluations based on the artefacts presented or POC (if called for) may lead to disqualification.

c) Bidder has to showcase above specifications / features and provide relevant document / declaration.

Declaration:

1. We hereby confirm that we have various certificates/bench mark testing standards for the items quoted to meet the intent of the Bid.

2. We hereby confirm that we have back to back arrangements with third party hardware software for providing continuous and un-interrupted support to meet SLAs obligations as per bid terms.

3. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.

Signature with seal:
Date
Name:
Designation :

केनरा बैंक Canara Bank

Amended Annexure-11

Technical Evaluation Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach and Attack Simulation Solution in Canara Bank for 3 years.

Ref: GeM Bid: GEM/2022/B/2885701 dated 27/12/2022.

The technical evaluation of the bidder will be carried as per the details furnished below:

Sl. No.	Criteria	Evaluation Parameters	Documents to be submitted	Max marks	Marks Obtained
1	The bidder having experience in handling the proposed Breach and Attack Simulation Tool & should be currently running in any organization in India for Application Services, Support, Administration, Management & Monitoring (POCs done will not be treated as experience of the bidder)	Experience of 2 years and above - 10 marks Experience of less than 2 years and above 1 years - 5 marks Experience of less than 1 years and above 6 months - 1 marks	Documentary evidence of contracts executed along with completion / undertaken certificate / invoices or any other document certifying that Project has been implemented successfully. Reference from customer along with customer contact details are required.	10	
2	The proposed Breach and Attack Simulation Tool should have been implemented & currently running in any BFSI organization in India for Application Services, Support, Administration, Management &	Per organization : 5 Marks	Documentary evidence of contracts executed along with completion / undertaken certificate / invoices or any other document certifying that Project has been implemented successfully.	25	

	Monitoring. (POCs done will not be treated as experience of the bidder)		Reference from customer along with customer contact details are required.		
3	Number of implementations of the proposed Breach and Attack Simulation Tool in any organization in India.	More than 3 BAS solution implementation experience in India - 10 marks 1 to 3 BAS solution implementation experience in India - 5 marks	Documentary evidence of contracts executed along with completion / undertaken certificate / invoices or any other document certifying that Project has been implemented successfully. Reference from customer along with customer contact details are required.	10	
4	The bidder / OEM experience in complying B. Functional requirement as per Annexure 2	Bidders should fulfill and implement the functional requirement as mentioned in Annexure 2 of the RFP.	The bidder in coordination with OEM has to conduct a presentation as part of Technical evaluation highlighting the capabilities as per the requirement of the Bank. Bidder in coordination with OEM has to submit the documentary evidence/self-declaration post presentation as a part of compliance to	50* *(Mark obtained as per Annex 2 will be proportionally adjusted) (X/81*50)	

D.I.T. Wing, Procurement Group CANARA BANK H.O., Bengaluru-560 001

			the functional requirement. The same needs to be validated. Bank may call for a PoC for demonstration of the functionalities.		
5	Availability of Solution certified manpower on payroll of the bidder/OEM.	10 resources and above in India - 5 Marks 5 resources and above and Less than 10 resources in India - 2 marks	Declaration from the company secretary/ HR Head to this effect.	5	
6	**Total Marks**			**100**	

* **The bidder should score minimum 75% of marks out of 100 marks for qualifying under Technical Evaluation along with compliance to all other terms and conditions. The bidders qualified under Technical Evaluation will be eligible for commercial opening.**

Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this GeM bid is liable for rejection.

Date

Signature with seal:
Name :
Designation :

*******************End of the Corrigendum-2*********************