Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
1	3	A. BID SCHEDULE & ABBREVIATIONS	Pre-bid Meeting Date & Time	1. Pre-bid meeting will be held on 11/09/2020, Friday at 3.30 pm Venue: Canara Bank, Second Floor, Conference Hall, DIT Wing-HO (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001. 2. Pre bid queries should be submitted as per Appendix-D. 3. Pre-bid Queries to E-mail hoditapm@canarabank.com must reach us on or before 09/09/2020, Wednesday at 3.00pm. Subject of the email should be given as "Pre Bid Queries for RFP 13/2020-21 dated 02/09/2020". Queries reaching after 3.00pm on 09/09/2019 will not be entertained.	Due to current situation, please organize a online meeting for the pre-bid meeting with 3 (three) participants per vendor	Kinidy refer the Amendment-1 to this RFP.
2	3	A. BID SCHEDULE & ABBREVIATIONS	9. Last Date, Time and Venue for Submission of Bids	23/09/2020, Wednesday upto 3.00pm Venue: Canara Bank, First Floor, DIT Wing-HO (Annex), Naveen Complex, 14 M G Road, Bengaluru 560001.	1. Can we consider online submission at this COVID restriction time? 2. Please consider atleast 3 weeks from the date of clarification responses - Please consider 7th Oct 2020 as the submission time?	Kinidy refer the Amendment-1 to this RFP.
3	10	B. INTRODUCTION	4. Objective	4.1. The solution should be able to simulate the latest attacks on the email gateway, web gateway and on endpoints present in the bank.	Does solution should also cover WEB application firwall attacks OR not ? Many places its mentioned cloud INFRA. Does cloud INFRA cover WAF Attack or not ?	The solution should be able to do the assessment on WAF & cloud infra (which includes the complete cloud components) also along with other areas mentioned in the RFP
4	10	B. INTRODUCTION	5. Requirement Details	Item details Number of License Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach and Attack Simulation Solution as per Annexure-7 & Annexure-8. ------------------ 5	Kindly clarify what is meant by Number of licenses 5 ? Does that mean it is to be deployed at 5 different locations	The solution has to do complete assessment as per point no 53 under Annexure-7 of this RFP.
5	12	B. INTRODUCTION	11. Training	11.1. The Bidders shall provide training by OEM to the identified Bank personnel / team on solution or features / service architecture, and functionality during and after implementation. The solution working should be demonstrated to the IT & Information Security Management and staff of the Bank after completion of the implementation and the review and feedback should be implemented. Bidder has to arrange the onsite-classroom training with workstations and required necessary amenities to facilitate the training. Trainer should be well experienced and must have industry certification. Location of the Training must be in Bengaluru only. Bidder should provide the training material and hands-on during the training.	Training can be conducted at Bank's premises but request bank to provide the required workstation and place to conduct the training. Remarks: It will be logistics nightmare to arrange at your premises if not provided with the infrastrucutre required.	Bidder has to comply with the RFP terms.

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

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
6	12	B. INTRODUCTION	11. Training	11.1. The Bidders shall provide training by OEM to the identified Bank personnel / team on solution or features / service architecture, and functionality during and after implementation. The solution working should be demonstrated to the IT & Information Security Management and staff of the Bank after completion of the implementation and the review and feedback should be implemented. Bidder has to arrange the onsite-classroom training with workstations and required necessary amenities to facilitate the training. Trainer should be well experienced and must have industry certification. Location of the Training must be in Bengaluru only. Bidder should provide the training material and hands-on during the training.	Training must be in Bengaluru only - (page 12/Clause 11.1) What if the current pandemic situation prevails and the travel restrictions are applicable. Since the trainers may have to fly from overseas	Bidder has to comply with the RFP terms.
7	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	**1.3. Installation Schedule:** 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations.	Kindly provide the list of locations	It will be implemented in DC & DR of the bank. Location / address will be provided to the seleted bidder.
8	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	**1.4. Project Timelines:** 1.4.4. Phase-1 (UAT and DR Implementation): The Bidder has to ensure installation and complete working of the solution within 7 weeks of acceptance of Purchase Order in the DR setup of the bank. The successful bidder has to complete the implementation of all the functionalities defined elsewhere in the RFP.	Why solution is required in DR ? When its not a Must have solution but On demand solution	Bidder has to comply with the RFP terms.
9	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	**1.2. Delivery Schedule is as follows:** **1.2.1. Supply of Hardware & other Items (including OS):** Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier. **1.2.2. Supply of Breach & Attack Simulation Solution:** Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier.	We request to extend the delivery timelines from 6 weeks to 8 weeks	**The RFP Clause is modified as under:** "**1.2.1. Supply of Hardware & other Items (Including OS):** Within **Seven (7) weeks** from the date of acceptance of Purchase Order or **Eight (8) weeks** from the date of issue of Purchase Order whichever is earlier. **1.2.2. Supply of Breach & Attack Simulation Solution:** Within **Seven (7) weeks** from the date of acceptance of Purchase Order or **Eight (8) weeks** from the date of issue of Purchase Order whichever is earlier."

D.I.T. Wing, Procurement
CANARA BANK
H.O., Bengaluru-560002

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
10	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.3. Installation Schedule: 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations. 1.3.2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution: The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Breach & Attack Simulation Solution at the bank branch/office within 2 weeks from the date of delivery of Breach & Attack Simulation Solution for each ordered locations.	We request to extend the delivery timelines from 2 weeks to 4 weeks	Bidder has to comply with the RFP terms.
11	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.2. Delivery Schedule is as follows: 1.2.1. Supply of Hardware & other Items (including OS): Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier.	Request Bank to Amend the clause as Supply of handware and OS within 8 weeks of Acceptance of the PO. Remarks: From ordering to import will usually take 8 weeks from the acceptance of PO	The RFP Clause is modified as under: "1.2.1. Supply of Hardware & other Items (including OS): Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier."

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
12	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.3. Installation Schedule: 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations. 1.3.2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution: The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Breach & Attack Simulation Solution at the bank branch/office within 2 weeks from the date of delivery of Breach & Attack Simulation Solution for each ordered locations.	Request Bank to amend the time line to 4 weeks from the date of delivery of Hardware and software. Remarks: From delivery acceptance and Hardware readiness will take minimum 4 weeks	Bidder has to comply with the RFP terms.
13	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.2. Delivery Schedule is as follows: 1.2.1. Supply of Hardware & other items (including OS): Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier.	Request to change the delivery shedule to 10 weeks from Date of accepting the PO	The RFP Clause is modified as under: "1.2.1. Supply of Hardware & other items (including OS): Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier."
14	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.2. Delivery Schedule is as follows: 1.2.1. Supply of Hardware & other items (including OS): Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Six weeks from the date of acceptance of Purchase Order or Seven weeks from the date of issue of Purchase Order whichever is earlier.	Request to change the delivery shedule to 10 weeks from Date of accepting the PO	The RFP Clause is modified as under: "1.2.1. Supply of Hardware & other items (including OS): Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier. 1.2.2. Supply of Breach & Attack Simulation Solution: Within Seven (7) weeks from the date of acceptance of Purchase Order or Eight (8) weeks from the date of issue of Purchase Order whichever is earlier."

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
15	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.3. Installation Schedule: 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations. 1.3.2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution: The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Breach & Attack Simulation Solution at the bank branch/office within 2 weeks from the date of delivery of Breach & Attack Simulation Solution for each ordered locations.	Request to change the implementation and integration and commisioning timelines to 4 weeks from date of Delviery	Bidder has to comply with the RFP terms.
16	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.3. Installation Schedule: 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations. 1.3.2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution: The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Breach & Attack Simulation Solution at the bank branch/office within 2 weeks from the date of delivery of Breach & Attack Simulation Solution for each ordered locations.	Request to change the implementation and integration and commisioning timelines to 4 weeks from date of Delivery	Bidder has to comply with the RFP terms.
17	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	**1.4. Project Timelines:** **1.4.4. Phase-1 (UAT and DR implementation):** The Bidder has to ensure installation and complete working of the solution within 7 weeks of acceptance of Purchase Order in the DR setup of the bank. The successful bidder has to complete the implementation of all the functionalities defined elsewhere in the RFP.	Request to change the phase 1 timelines to 16 weeks from date of accepting the PO	**The RFP CLause is modified as under:** **1.4.4. Phase-1 (UAT and DR implementation):** The Bidder has to ensure installation and complete working of the solution within **Nine (9) weeks** of acceptance of Purchase Order in the DR setup of the bank. The successful bidder has to complete the implementation of all the functionalities defined elsewhere in the RFP.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
18	13	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.3. Installation Schedule: 1.3.1. Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS): The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Hardware and other items at the bank branch/office within 2 weeks from the date of delivery of all the materials for each ordered locations. 1.3.2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution: The successful bidder should ensure installation, configuration, integration and commissioning of the delivered Breach & Attack Simulation Solution at the bank branch/office within 2 weeks from the date of delivery of Breach & Attack Simulation Solution for each ordered locations.	We request Bank to modify as 4 weeks from the date of delivery	Bidder has to comply with the RFP terms.
19	14	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	2. Security	2.2. The Bank will not provide any remote session and direct internet connectivity to the equipment in terms of support which may leads to the vulnerability of the system.	How can testing of attack be done if there is no internet connectivity ?	Bidder has to comply with the RFP terms.
20	14	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	1. Delivery, Installation, Integration and Commissioning	1.4. Project Timelines: 1.4.5. Phase-2 (DC Implementation and Go Live): After successful completion of DR implementation, the selected Bidder should complete the roll out of the entire solution in the DC setup of the bank within 8 weeks of acceptance of the Purchase Order.	Request to change the phase 2 timelines to 18 weeks from date of accepting the PO	The RFP CLause is modified as under: "1.4.5. Phase-2 (DC implementation and Go Live): After successful completion of DR implementation, the selected Bidder should complete the roll out of the entire solution in the DC setup of the bank within Ten (10) weeks of acceptance of the Purchase Order."
21	14	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	2. Security	2.2.. The Bank will not provide any remote session and direct internet connectivity to the equipment in terms of support which may leads to the vulnerability of the system.	Bank will not provide any remote sessions and direct internet connectivity to the equipment in terms of support which may leads to vulnerability.- (Page 14 /Clause 2.2) How will the TAC troubleshoot over remote in case of any technical issue arise. ?	Bidder has to comply with the RFP terms.
22	15	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	3. Acceptance	3.1. Bank will evaluate the offered Solution implemented by the bidder. If the Solution experiences no failures and functions according to the requirements of the RFP as determined by the Bank during the implementation period, then the solution will be accepted by the Bank and the project will be considered as deemed signed-off.	We understand that the acceptance criteria for the solution shall be mutually agreed. The solution should be accepted as soon as it meets the acceptance criteria. We does not warrant error free or uninterrupted service or fitness for a particular purpose	Bidder has to comply with the RFP terms.
23	15	Annexure-7	Sizing of Hardware including Software/OS for DC & DRC	1. Quoted Hardware/Software/OS details for Development Environment in both DC & DRC:	Details of Web, Apps, DB Servers and storage are not mentioned.	Bidder has to specify the detail which is required for the implementation of the project

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
24	16	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	Whole Clause	We seek to clarify that the LD amount or percentage shall be mutually agreed and shall be levied only if We is directly and solely liable and subject to overall liability cap. Bidder seeks to clarify that Bank may invoke the BG only if any failure on Bidder's part amounts to a material breach which remains uncured even after a notice of 30 days.	Bidder has to comply with the RFP terms.
25	16	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	5.1. Penalties/Liquidated damages for delay in Delivery of Hardware and Solution/Software would be as under: 5.1.1. Non-compliance of the Supply/delivery as per clause 1.2.1 will result in imposing penalty of 0.50% on delay in delivery per week or part thereof plus GST by the Bank on the invoice value of Hardware items (including OS) (exclusive of Taxes) location/office address wise. 5.1.2. Non-compliance of the Supply/delivery of Breach & Attack Simulation Solution as per clause 1.2.2 will result in the imposing penalty of 0.50% on delay in delivery per week or part thereof plus GST by the Bank on the invoice value of Breach & Attack Simulation Solution (exclusive of Taxes) location/office address wise. 5.1.3. However, the total Penalty/LD to be recovered under clause 5.1.1 & 5.1.2 shall be restricted to 5% of the total value of the order (exclusive of Taxes) plus GST.	We requests overall penalties (inclusive of LD, SLA penalties, penalties during AMC etc) to be capped at 10% of the TCV.	Bidder has to comply with the RFP terms.
26	16	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	Whole Clause	Overall project completion penalty should be capped at a mutually agreement %.	Bidder has to comply with the RFP terms.
27	16	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	5.3. Penalties/Liquidated damages for not maintaining uptime: 5.3.2. The maximum penalty levied shall not be more than the 5% of invoice value (plus GST) during warranty period and 50% of AMC / ATS amount payable for one year (plus GST) during AMC/ATS period.	request to change the Maximum penalty levied shall not be more than the 3% of invoice value during warranty period and 10% of AMC /ATS amount payable for one year (Plus GST)	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
28	16	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	**5.3. Penalties/Liquidated damages for not maintaining uptime:** 5.3.1. If the bidder fails to maintain the guaranteed Uptime during Warranty and ATS period (if contracted), the penalty for Uptime will be deducted as under: Level of availability calculated on monthly basis Penalty Amount 98.00% to 100% No penalty 97.00% to 97.99% 0.05% on total order value for every hour or part thereof. 96.00% to 96.99% 0.10% on total order value for every hour or part thereof. 95.00% to 95.99% 0.15% on total order value for every hour or part thereof. Less than 95.00% 0.50 on total order value for every hour or part thereof.	We request the bank to amend this to 0.05% of annual contract value	Bidder has to comply with the RFP terms.
29	17	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	5.4. Any financial loss to the Bank on account of fraud taking place due to Successful Bidder, its employee or their services provider's negligence shall be recoverable from the Successful Bidder along with damages if any with regard to the Bank's reputation and goodwill.	Please clarify if the clause intends to cover indirect damages. We do not take liability for indirect damages, loss of goodwill or lost profits.	Bidder has to comply with the RFP terms.
30	17	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	5.5. Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions directly attributable to the staff of the Bidder.	We understand that this clause intends to cover only direct damages subject to overall mutually agreed liability cap	Bidder has to comply with the RFP terms.
31	17	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	5.8. All the above LDs are independent of each other and are applicable separately and concurrently.	Bank is requested to clarify this.	Bidder has to comply with the RFP terms.
32	17	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	5. Penalties/Liquidated Damages	**5.3. Penalties/Liquidated damages for not maintaining uptime:** 5.3.4. If monthly uptime is less than 95% in three consecutive months, bank may at its sole discretion blacklist the bidder in addition to imposing penalty and invoking the bank guarantee.	Kindly remove the highlighted portion with regards to blacklisting, as the Bank already has the right to levy penalty, invoke BG and terminate the contract.	Bidder has to comply with the RFP terms.
33	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	Sl. No. Payment Stage % of Payment 3. After Completion of Warranty Period (i.e. three year). Warranty period will start from the date of acceptance of solution by the Bank.- 10% of the Invoice Value of these Hardware for Breach & Attack Simulation solution with required OS, Database License and other Licenses Or On submission of BG equivalent to warranty payment.	In case it's a annual subscription, it will be subscription amount	Bidder has to comply with the RFP terms.

D.I.T. Wing, Procurement
CANARA BA
H.O., Bangalore 560 001

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
34	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	6.2. Payment schedule for Breach & Attack Simulation Solution will be as under: Sl. No. Payment Stage % of Payment 1. Delivery of Breach & Attack Simulation Solution as per clause 1.2.2 40% of the Invoice Value of Breach & Attack Simulation Solution. 2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution as per clause 1.3.2 40% of the Invoice Value of Breach & Attack Simulation Solution. 3. Escrow agreement 10% of the invoice value will be released after signing Escrow Agreement and depositing of source code. 4. After Completion of Warranty Period (i.e. three year). Warranty period will start from the date of acceptance of solution by the Bank. 10% of the Invoice Value of Breach & Attack Simulation Solution Or On submission of BG equivalent to warranty payment. 5. ATS for Breach & Attack Simulation Solution Quarterly in Arrears	Please clarify the need for escrow agreement and what would be the trigger. How would an escrow agent be selected and when.	Kinldy refer the Amendment-1 to this RFP.
35	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	Whole Clause	We seeks deletion of the existing clause in its entirety and substitute it with the following clause: Payments are due from date of receipt of invoice and payable within thirty (30) days of date of invoice issued to customer. In the event of late payments, We reserves the right to charge a late payment fee @ 2% per month on the overdue amounts, in addition to the right of suspension of services, till the overdue amounts are paid. We proposes the following payment schedule: (a) Products: 100% on delivery; and (b) Implementation Services: 100% on completion; and (c) Support services: Yearly and in advance.	Bidder has to comply with the RFP terms.
36	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	AMC for required hardware for Breach & Attack Simulation solution with required OS ,Database licence , and other licences	Request to change the payment terms to Yearly in advance	Bidder has to comply with the RFP terms.
37	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	ATS for Breach and Attack solution	Request to change the payment terms to Yearly in advance	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
38	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	The following terms of payment shall be applicable to this contract and will be released after execution of Contract Agreement: 6.1. Payment schedule for Required Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses will be as under: Sl. No. Payment Stage % of Payment 1. Delivery of Required Hardware for Breach & Attack Simulation solution with required OS, Database License and other Licenses as per clause 1.2.1 40% of the Invoice Value of these Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses 2. Installation, Configuration, Integration and Commissioning of Hardware Appliance/Items (including OS Database License and other Licenses) as per clause 1.3.1 50% of the Invoice Value of these Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses 3. After Completion of Warranty Period (i.e. three year). Warranty period will start from the date of acceptance of solution by the Bank. 10% of the Invoice Value of these Hardware for Breach & Attack Simulation solution with required OS, Database License and other Licenses Or On submission of BG equivalent to warranty payment	We request this to be amended to industry standard of 70% on delivery, 20% on Install and 10% on production of a BG for equivalent amount	Bidder has to comply with the RFP terms.
39	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	The following terms of payment shall be applicable to this contract and will be released after execution of Contract Agreement: 6.1. Payment schedule for Required Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses will be as under: Sl. No. Payment Stage % of Payment 1. Delivery of Required Hardware for Breach & Attack Simulation solution with required OS, Database License and other Licenses as per clause 1.2.1 40% of the Invoice Value of these Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses 2. Installation, Configuration, Integration and Commissioning of Hardware Appliance/Items (including OS Database License and other Licenses) as per clause 1.3.1 50% of the Invoice Value of these Hardware for Breach & Attack Simulation Solution with required OS, Database License and other Licenses 3. After Completion of Warranty Period (i.e. three year). Warranty period will start from the date of acceptance of solution by the Bank. 10% of the Invoice Value of these Hardware for Breach & Attack Simulation solution with required OS, Database License and other Licenses Or On submission of BG equivalent to warranty payment	We request this to be amended to Yearly in Advance	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
40	18	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	6. Payment Terms	6.2. Payment schedule for Breach & Attack Simulation Solution will be as under: Sl. No. Payment Stage % of Payment 1. Delivery of Breach & Attack Simulation Solution as per clause 1.2.2 40% of the Invoice Value of Breach & Attack Simulation Solution. 2. Installation, Configuration, Integration and Commissioning of Breach & Attack Simulation Solution as per clause 1.3.2 40% of the Invoice Value of Breach & Attack Simulation Solution. 3. Escrow agreement 10% of the invoice value will be released after signing Escrow Agreement and depositing of source code. 4. After Completion of Warranty Period (i.e. three year). Warranty period will start from the date of acceptance of solution by the Bank. 10% of the Invoice Value of Breach & Attack Simulation Solution Or On submission of BG equivalent to warranty payment. 5. ATS for Breach & Attack Simulation Solution Quarterly in Arrears	We request this milestone to be deleted	Bidder has to comply with the RFP terms.
41	19	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	7. Support	7.2. Support should include advising & helping the Bank in implementing controls for the risk advised by regulators/Govt. Of India.	Bidder would be providing advices and resolution lies with end application/device owner. Please clarify	Bidder has to comply with the RFP terms.
42	19	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	7. Support	7.5. The Bidder should help Bank in resolving any security observations as per the IS policy of the Bank.	Bidder shall be assisting in providing documents, changes on end solution/device. Implemneting the soluiton or changes to end soluiotn or devices woule be Banks responsibility.	Bidder has to comply with the RFP terms.
43	20	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	9. Warranty	9.11. The bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship. Bidder must warrant all components, accessories, spare parts etc. against any manufacturing defects during the warranty period.	Bank to clarify if the intention is to make bidder liable for third party OEM warranties. We seeks to clarify that We does not warrant third party products.	Bidder has to comply with the RFP terms.
44	22	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	13. Subcontracting	The selected vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.	Bank to kindly confirm that such consent will not be unduly withheld.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
45	22	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	14. Defect liability	In case any of the supplies and equipment delivered under the Contract are found to be defective as to material and workmanship and / or not in accordance with the requirement, and/or do not achieve the guaranteed performance as specified herein, within the warranty and AMC period (if contracted) of the contract, the Bidder shall forthwith replace/make good such defective supplies at no extra cost to the bank without prejudice to other remedies as may be available to the bank as per RFP terms.	All warranty/replacements is as per OEM warranty terms & conditions only. Kindly delete the same.	Bidder has to comply with the RFP terms.
46	23	D. BID PROCESS	7. Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD	7.5.2. If the selected bidder fails to accept the purchase order within 7 days or fails to sign the contract or fails to furnish performance guarantee in accordance with the terms of the RFP.	We presume clause 7.5.2 will only be applicable if both the Parties have mutually discussed and agreed on all the terms and conditions by signing the contract thereto and in case Bidder fails to accept the PO pursuant to signing of the Contract by both the Parties. Please confirm.	Bidder has to comply with the RFP terms.
47	23	D. BID PROCESS	13. Assumptions/Presumptions/Modifications	The Bank would like to expressly state that any assumption, presumptions, modifications, terms, conditions, deviation etc., which the bidder includes in any part of the Bidder's response to this RFP, will not be taken into account either for the purpose of evaluation or at a later stage, unless such assumptions, presumptions, modifications, terms, conditions deviations etc., have been accepted by the Bank and communicated to the bidder in writing. The bidder at a later date cannot make any plea of having specified any assumption, terms, conditions, deviation etc in the bidder's response to this RFP document. No offer can be modified or withdrawn by a bidder after submission of Bid/s.	Kindly confirm that Bank will be considering the deviations submitted by the bidder and a contract will be signed only on mutually agreed terms. Please confirm that EMD shall not be forfieted if parties fail to agree to terms.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
48	29	F. Ownership & Awarding of Contract	6. Effective Date 8. Security Deposit / Performance Bank Guarantee 9. Execution of Agreement	Please refer to the section in the RFP	Cl. 6 Suggests that effective date will be date of acceptance of the order by the bidder which may be required to be accepted by the Bidder within 7 days from the date of receipt of order. We presume that acceptance as mentioned herein will be subject to both the Parties having mutually agreed to all the terms and conditions. Please confirm. Cl. 8 Security Deposit: The current clause allows customer to forfeit PBG if the Bidder fails to complete obligations under the contract. This clause is very broad. PBG shall be forfeited only in case of a material breach by We which remains uncured even after a notice of 30 days. Cl. 9.1: While we are in principle agreement with this clause we are presuming that any signing of agreement will be subject to mutual discussion and agreement and in case there is no agreement between the Contracting parties then either party should be allowed to walk away from contracting without any implications whatsoever. Accordingly, we will also request you to remove reference to forfeiture of EMD. Cl. 9.2 & 9.3: We presume that our proposal will also form part of the final contractual documents.	Bidder has to comply with the RFP terms.
49	29	F. Ownership & Awarding of Contract	11. Order Cancellation/Termination of Contract	Whole Clause	To begin with It is understanding that by using the term cancel customer is intending to suggest termination. Please confirm. Additionally, Please note that with respect to Cl. 11.1 the reason for termination as provided therein is for cause. Accordingly, kindly request you to issue a notice of not less than 60 days before initiating termination. Additionally, we also presume that termination will only be invoked in case the service provider is unable to cure the breach within a reasonable period. As for Cl. 11.2; subclauses 11.2.2, 11.2.3 & 11.2.6 are already coverer under Cl. 11.1. Accordingly request deletion of the same. The rest of clauses provided therein please issue a notice of not less than 60 days before initiating termination. Separately, in both instances of termination as mentioned above, we presume that We will be paid for all the services rendered and deliverables delivered until the effective date of termination. Please confirm. Cl. 11.4 & 11.5: Given that the intent under both these clauses are the same, request you to kindly merge this as one. Additionally, it is also our	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
50	30	G. GENERAL CONDITIONS	2. Roles & Responsibility during Project Implementation	2.3. In case of any damage of Bank's property during execution of the work is attributable to the bidder, bidder has to replace the damaged property at his own cost.	We understand that this clause intends to cover only direct damages subject to overall all mutually agreed liability cap	Bidder has to comply with the RFP terms.
51	30	G. GENERAL CONDITIONS	4. Human Resource Requirement	4.6. The Bidder shall extend all of the outsourced banking and financial services by deploying such personal that have high integrity and meet the qualifications and other criteria stipulated by the Reserve Bank of India , Government or the Bank from time to time and agrees and undertake that during the subsistence of this agreement they will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time ,as per the provisions of Minimum Wages Act 1948.	We seek clarity on the clause. Does it apply to the scope of the RFP?	Bidder has to comply with the RFP terms.
52	30	G. GENERAL CONDITIONS	5. Responsibility for Completeness	5.1. The bidder shall ensure that the Solution provided [Hardware/Software etc] meets all the technical and functional requirements as envisaged in the scope of the RFP. 5.2. The bidder shall deliver, install, configure the supplied Solution as per Technical specification and Scope of Work described elsewhere in the RFP and arrange for user level demo at bidder's cost as per accepted time schedules. The bidder is liable for penalties levied by Bank for any deviation in this regard. The bidder shall provide for all drivers/software required to install, customize and test the system without any further charge, expense and cost to Bank. 5.3. The Bidder shall be responsible for any discrepancies, errors and omissions or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The bidder shall take all corrective measures arising out of discrepancies, error and omission other information as mentioned above within the time schedule and without extra cost to the bank.	We seeks the Bank to clarify that the scope of work, specifications will be as mutually agreed by the parties in the bid response document and mutually agreed deviations. Further We understand that penalty if any will be as mutually agreed under the RFP and Bid response documents and will be subject to overall liablity cap and We will be liable only for direct damages	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
53	30	G. GENERAL CONDITIONS	6. Inspection of Records	Bank at its discretion may verify the accounts and records or appoint third party for verification including an auditor for audit of accounts and records including Hardware, Software & other items provided to the Bank under this RFP and the vendor shall extend all cooperation in this regard.	While we are in principle agreement with this clause it is our understanding that such audits shall be conducted only to verify if Bidder is performing services in accordance with the service levels. Any third party auditor may be appointed only with the mutual consent of the parties on a non-contingent basis after he has executed a confidentiality agreement with the Bidder. Further, we understand that the Bidder will not be obligated to share any information relating to Bidder's costs, Bidder proprietary data, confidential information of Bidder's other customers and internal audit reports of the Bidder. Such audit shall be conducted (a) upon thirty days prior written notice to Bidder; (b) no more than once each calendar year; (c) only in relation to the previous twelve months' activities; (d) during normal business hours; and (e) to the extent it does not interfere with Bidder's ability to perform the Services in accordance with the Agreement. Please clarify.	Bidder has to comply with the RFP terms.
54	30	G. GENERAL CONDITIONS	7. Negligence	In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.	We understands that this clause intends to cover only direct damages subject to overall mutually agreed liability cap. Please confirm. We wishes to clarify that We's liability will be solely for matters for which it is directly and solely liable. Also, that Bank would terminate only after reasonable notice period and opportunity to cure and We would be paid for services rendered upto the effective date of termination. Also, We seeks deletion of the word "cancellation". Any dispute with respect to the work shall be referred to the dispute resolution mechanism before termination	Bidder has to comply with the RFP terms.
55	30	G. GENERAL CONDITIONS	8. Assignment	8.1. The vendors shall not assign to any one, in whole or in part, its obligations to perform under the RFP/contract, except with the Bank's prior written consent. 8.2. If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the Vendor under this RFP.	Request the clause to be made mutual. Accordingly, we propose the following clause: Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other. Assignment of We rights to receive payments or assignment by We in conjunction with the sale of the portion of We's business that includes a product or service is not restricted.	Bidder has to comply with the RFP terms.
56	30	G. GENERAL CONDITIONS	12. Intellectual Property Rights	Whole Clause	Bidder requests that the indemnity in this clause be to limited any third party infringement claim pertaining to Bidder owned products.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
57	30	G. GENERAL CONDITIONS	13. Confidentiality and Non-Disclosure	Whole Clause	While we are in principle agreement with this clause, we reckon that Bank would extend the same courtesy with respect to the information shared by We and protect such information in a manner as it would have protected its own confidential information. Separately, it is also our understanding that both the Parties will enter into a separate mutually acceptable NDA in case We were to be shortlisted as the final Vendor.	Bidder has to comply with the RFP terms.
58	30	G. GENERAL CONDITIONS	14. Indemnity	Whole Clause	Request you to kindly limit indemnities to court awarded damages for any third party claims only. Please confirm. Accordingly, we would like to confirm that We will be responsible for indemnity obligations as provided under Cl. 14.2 only in addition to any claims with respect to damage to real and tangible property, death or bodily injury. Request you to kindly remove reference to Cl. 14.1.1, 14.1.2 and 14.2.2. As for 14.3, while we are in principle agreement with this clause, it is also our understanding that We will not be responsible for any indirect and/or consequential damages including any loss of profit, loss of data and loss of reputation. Further, the liability cap as provided under this clause shall be the aggregate liability cap of the Bidder for any claims that may arise out of the Agreement and the only exclusions shall be in the context of death, damage to tangible property and bodily injury only.	Bidder has to comply with the RFP terms.
59	30	G. GENERAL CONDITIONS	17. Corrupt and Fraudulent practices	Whole Clause	Please note that we are in principle agreement with this clause. Accordingly, it is our understanding that any determination of We's involvement in any of the activities as provided under this Contract will be determined by an independent body such as a court of law before declaring We as a defaulter for the purposes of this clause. Please confirm.	Bidder has to comply with the RFP terms.
60	30	G. GENERAL CONDITIONS	19. Amendments to the Purchase Order	Whole Clause	While we are in principle agreement with this clause, it is our understanding that PO and terms provided therein are applicable only for administrative purposes and that neither party will be bound by the terms provided therein. Please confirm.	Bidder has to comply with the RFP terms.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru - 560 00

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
61	30	G. GENERAL CONDITIONS	7. Negligence	In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.	Bank to kindly confirm that any cancellation or termination of contract will be done only after giving 30 days written notice to the Bidder to cure or remedy the default and only upon failure of the Bidder to remedy or cure such default.	Bidder has to comply with the RFP terms.
62	30	G. GENERAL CONDITIONS	10. Insurance	The Hardware to be supplied will be insured by the bidder against all risks of loss or damages from the date of shipment till such time, the same is delivered and installed at site and handed over to the Bank/Office. The Bidder has to obtain transit insurance cover for the items to be delivered from their factory/godown to the location and such insurance cover should be available till installation of the Solution. If there is any delay in the installation which could be attributed to Bank, in such an event the insurance must be available for minimum 30 days from the date of delivery of Solution.	Bank to confirm that the Insurance provided for the Hardware would be transit insurance till the point of delivery.	Bidder has to comply with the RFP terms.
63	30	G. GENERAL CONDITIONS	11. Guarantees	The bidder should guarantee that the hardware items delivered to the Bank are brand new, including all components. In the case of software, the bidder should guarantee that the software supplied to the Bank includes all patches, updates etc., and the same are licensed and legally obtained. All hardware and software must be supplied with their original and complete printed documentation.	Bank to confirm that all hardware & software to be supplied comes with the OEM/Software Licensor guarantee.	Bidder has to comply with the RFP terms.
64	30	G. GENERAL CONDITIONS	12.Intellectual Property Rights	Whole Clause	We request that provisions related to Indemnity be restricted to Third party indemnification claims arising from infringement of IPR in respect of the Services provided by Bidder.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
65	30	<u>G. GENERAL CONDITIONS</u>	12.Intellectual Property Rights	Whole Clause	We request the below modifications to Clause 14- Indemnity Clause from the General Terms & Conditions: 14.1 The Bidder shall keep the Bank indemnified against claims (including reasonable legal costs) which may be caused to or suffer by or made or taken against the Bank arising out of: 14.1.1 Statutory and/or regulatory claims, suits, actions or proceedings against the Bank arising directly from Bidder's breach (or alleged breach) of applicable tax initiated by an appropriate governing body or authority. 14.2 The bidder shall keep the Bank indemnified against 3rd party IPR claims leading to court awarded damages against the Bank from infringement of any law pertaining to patents, trademarks, copyrights etc. in respect of the Services provided by the Bidder: 14.2.1 All indemnities shall survive notwithstanding expiry or termination of the contract. 14.2.2 the limits specified in above clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual Property Rights. For claims relating to fraudulent misrepresentation, bodily injury or death arising from bidder's	Bidder has to comply with the RFP terms.
66	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	<u>Eligibility Criteria:</u> The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. <u>Documents to be submitted:</u> The Bidder has to provide reference letter from their Customers to this effect.	Along with customer reference letters, We request Bank to accept only copies of purchase order / work orders / any other form of signed contract document as well.	<u>The Eligibility Criteria is amended as under:</u> "**Eligibility Criteria:** 5. The **<u>Bidder/OEM</u>** should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
67	35	Annexure-2	Eligibility Criteria Declaration Criteria no.6	<u>Eligibility Criteria:</u> The proposed Breach and Attack Simulation solution should have been [not necessarily by the bidder] implemented and currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. <u>Documents to be submitted:</u> The Bidder has to provide reference letter duly mentioning the solution name from the Customers to this effect.	Along with customer reference letters, We request Bank to accept only copies of purchase order / work orders / any other form of signed contract document as well.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
68	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	Eligibility Criteria: The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. Documents to be submitted: The Bidder has to provide reference letter from their Customers to this effect.	The Bidder should have implemented Breach and Attack Simulation Solution/Any 3 IT Security Solutions and it should be currently running in any of the BFSI Sector organization Globally or any listed company /Government / PSU Organization in India. **Remarks:** As this is a new solution and most of the customers yet to implement this	The Eligibility Criteria is amended as under: "Eligibility Criteria: 5. The Bidder/OEM should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
69	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	Eligibility Criteria: The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. Documents to be submitted: The Bidder has to provide reference letter from their Customers to this effect.	Please consider Bidder/OEM here. Can the bidder submit OEM credentials to address/ suffice this criteria? Since MAF will ensure back to back and guaranteed delivery for canara bank. This will help you receive bids from as many OEM players and not restricting to bidders participating Due to participation methology, each OEM can place one bid only and this will help more OEM to participate who dont have hardware experience	The Eligibility Criteria is amended as under: "Eligibility Criteria: 5. The Bidder/OEM should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
70	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	Eligibility Criteria: The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. Documents to be submitted: The Bidder has to provide reference letter from their Customers to this effect.	Please consider Bidder/OEM here. Many eligible OEM players do not have hardware experience in India and this clause restricting bidders to having implementation experience will give Canara bank lesser options in terms of OEM to select from. Please take MAF and consider bidder/OEM for this clause.	The Eligibility Criteria is amended as under: "Eligibility Criteria: 5. The Bidder/OEM should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
71	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	Eligibility Criteria: The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. Documents to be submitted: The Bidder has to provide reference letter from their Customers to this effect.	Since this is a new area/ solution field, please consider OEM experience as bidder experience here. Please ensure broader participation to include all OEM's available today to get best price/ solution Due to participation methology, each OEM can place one bid only. Also MAF will ensure back to back and guaranteed delivery for canara bank	The Eligibility Criteria is amended as under: "Eligibility Criteria: 5. The Bidder/OEM should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
72	35	Annexure-2	Eligibility Criteria Declaration	5. The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. The Bidder has to provide reference letter from their Customers to this effect.	We request Bank to amend the clause below: The bidder/OEM should have implemented breach and attack simulation and should be currently running in any of the BFSI sector organization globally or any listed company/government/PSU organization in India or world wide	**The Eligibility Criteria is amended as under:** "**Eligibility Criteria:** 5. The **Bidder/OEM** should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
73	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	**Eligibility Criteria:** The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect.	We request you relax this criteria for much open participation to include the OEM or Bidder to facilitate this specification and further allow to participate, even if a similar solution is sold but yet to be implemented.	**The Eligibility Criteria is amended as under:** "**Eligibility Criteria:** 5. The **Bidder/OEM** should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."
74	35	Annexure-2	Eligibility Criteria Declaration Criteria no.6	**Eligibility Criteria:** The proposed Breach and Attack Simulation solution should have been [not necessarily by the bidder] implemented and currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter duly mentioning the solution name from the Customers to this effect.	We request you relax this criteria for much open participation to include the OEM or Bidder to facilitate this specification and further allow to participate, even if a similar solution is sold but yet to be implemented.	Bidder has to comply with the RFP terms.
75	35	Annexure-2	Eligibility Criteria Declaration Criteria no.5	**Eligibility Criteria:** The Bidder should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect.	This being relative new solution in the market Bidder does not have any reference. Hence request Bank to change as Bidder / OEM	**The Eligibility Criteria is amended as under:** "**Eligibility Criteria:** 5. The **Bidder/OEM** should have implemented Breach and Attack Simulation solution and should be currently running in any of the BFSI sector organization globally or any listed company/Government/PSU organization in India. **Documents to be submitted:** The Bidder has to provide reference letter from their Customers to this effect."

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
76	38	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	A. TECHNICAL REQUIREMENTS 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. c) Mozilla Firefox version 47 and above. 3. Java Runtime Environment 6u31 and above	Server Operating Systems are important also, can we add Windwos Server 2012R2,2016 and 2019 for assessment ?	Bidder has to comply with the RFP terms.
77	38	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 2. The simulation agent should be compatible on various platforms like Window, Linux, MAC OS etc.	You mean that to support different OS threats or spesifically install an agent on mac or linux ? May you change the sentence, "The simulation platform should support for testing linux,mac os and windows based attacks on network level."	We have to do the assessment on all the OS types & versions
78	38	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	Is the solution with the sample malware files need to run across the Canara Bank Computer Machines or in some sandboxed environment (or Test & Dev setup)	The decision will reside with the bank and would be provided to the selected bidder.
79	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	Threats needs to be validaded after become validated from various perspective.(Is there any exploit etc..) So to limit all threats with 1 day may not be the feasible. Kindly requesting to change thids closure " The solution should be able to source latest threats in the industry and sholud be able to provide immediately, for the critical threats. (48 h)	Bidder has to comply with the RFP terms.
80	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 16. Solution should be able to export and import malware samples/hashes etc.	Why do we need import option ? This option could be harmful without validating real threats.If possible can we change the clause to "Solution should be able to export and when requested vendor will implement the real threats after validating"	Bidder has to comply with the RFP terms.
81	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	Typically the BAS solutions focus on the specific attack methodology, hence it cannot suggest rules or configurations to be done at security solutions. Hence we would request bank to remove "if they were not able to detect then should be able to suggest rules/ configurations to be done on the security sections" This particular this portion from the clause.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
82	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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 day is too short for any OEM to release attacker TTP's, "We would request bank to modify it as at the earliest instead of 1 day" . At FireEye we release TTPs that are in line with industry standard frameworks such as OWASP, NIST and ATT&CK and we coverage typically address all known attacker behaviors. We are able to release ad-hoc TTPs as and when we notice a new behaviour that isn't already documented by OWASP, NIST or ATT&CK.	Bidder has to comply with the RFP terms.
83	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 6.The solution should identify controls specific effectiveness of models (MITRE, NIST etc.).	Is the validation of the security controls on the each Desktop across Canara Banks' Computers that need to be validated with Simulations or some specific sample machines in a sandbox environ as security posture of every desktop may vary owing to many dynamics across the volume of machines that may be installed across Canara Bank.	The decision will reside with the bank and would be provided to the selected bidder.
84	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	Is there any specific list of endpoint security controls whose effectiveness needs to be validated as otherwise it is difficult to assess the kinds of security controls that may be deployed across the entire Canara Bank endpoints	The decision will reside with the bank and would be provided to the selected bidder.
85	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	As there are various private/gov Global and Indian entities that are tracking the threats discovery across the Globe. We request you to specify the Entity/Agency against which the 1-day readiness of simulation use case is expected.	Bidder has to comply with the RFP terms.
86	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	As the agents/simulator are installed on the machines, the identification of the Network Configuration faults will require a Automated VAPT engines through add-on SaaS tools. Is Canara Bank OK with the SaaS based Tool(s) inclusion.	Bidder has to comply with the RFP terms.
87	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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.	Typically the BAS solutions focus on the specific attack methodology, hence it cannot suggest rules or configurations to be done at security solutions. Hence we would request bank to remove "if they were not able to detect then should be able to suggest rules/ configurations to be done on the security sections" This particular this portion from the clause.	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
88	39	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 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 day is too short for any OEM to release attacker TTP's, "We would request bank to modify it as at the earliest instead of 1 day" . At FireEye we release TTPs that are in line with industry standard frameworks such as OWASP, NIST and ATT&CK and we coverage typically address all known attacker behaviors. We are able to release ad-hoc TTPs as and when we notice a new behaviour that isn't already documented by OWASP, NIST or ATT&CK.	Bidder has to comply with the RFP terms.
89	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 18. The solution should be able to initiate Phishing email delivery to a client mailbox (Phishing email delivery test) with the capability of accessing the responses.	This is a pentest approach.In simulation environment we shouldn't touch company assets directly. Including people. Can we remove this clause ?	Bidder has to comply with the RFP terms.
90	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 22. The solution should be able to detect data transfer to and from malicious domains / IPs / websites (Secure web gateway / proxy test).	This clause needs more clarification.or you may change " The solution should be able to test malicious code download attacks for assessing proxies and secure web gateways"	Bidder has to comply with the RFP terms.
91	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 17. The solution should be able to do Email security assessment (improper configuration or implementation of email filters)	Suggested clause: The solutions should send real malicious emails to dedicated email accounts within the Bank to send threats, like malware and spear phishing links, and/or send sensitive information out of the bank's network to tests effectiveness of bank's email controls.	Bidder has to comply with the RFP terms.
92	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 19. Endpoint Assessment - test security state of endpoints by comprehensively testing regardless of the method used to do the assessment.	Suggested clause: "Endpoint Assessment- The solution should have the ability to execute destructive attacks and behaviours in a safe endpoint environment to validate kill chain behaviour". ----------------------------- Note: (Destructive malware attack simulation at end user machine will help bank to gauge the efficacy of the endpoint security deployed in the bank 's end user machines, this performs in a safe environment)	Bidder has to comply with the RFP terms.
93	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 25. 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.	Suggested clause: The solution should have the ability to execute destructive and non-destructive attacks safely in the bank's environment without spreading malware or infected files to other systems.	Bidder has to comply with the RFP terms.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 00

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
94	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 26. 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.	Suggested clause: The solution should have the ability to identify the exact response provided by security controls and validate them against measures such as block, detect, log, alert or missed and map how hosts interact with files, including malware, across endpoint environment. (eg: if the file transfer was blocked by firewall or if the file was quarantined by antivirus or detected by EDR)	Bidder has to comply with the RFP terms.
95	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 28. The solution should be able to generate detailed report covering the attacks which were successful and should detail the indicators of compromise (loCs) and how the attack played out in the environment.	Suggested clause: The solution should be able to generate detailed report covering the attacks which were successful and should have the detail of the TTP's and behaviors on how the attack played out in the environment (Attacker TTP's are more powerful than the IOC's)	Bidder has to comply with the RFP terms.
96	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 21.The solution should be able to simulate access, connection or data transfer attempt while performing Network segmentation test.	As the agents/simulator are installed on the machines, the identification of the Network Configuration faults will require a Automated VAPT engines through add-on SaaS tools. Is Canara Bank OK with the SaaS based Tool(s) inclusion.	Bidder has to comply with the RFP terms.
97	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 20.The solution should be able to perform privilege escalation during endpoint assessment .	Is the solution expected to perform the Simulation of the Privilege Escalation use case once pivoted or expected to perform a Privilege Escalation with success on machines across the bank computer machines, as this may not be feasible with the kind of security controls deployed across the Canara Bank Computer machines.	Bidder has to comply with the RFP terms. However, the decision will be taken by the Bank during simulation.
98	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 28.The solution should be able to generate detailed report covering the attacks which were successful and should detail the indicators of compromise (loCs) and how the attack played out in the environment.	Which all Cyber Observables (IP, Domain Name, CnC, Bitcoin Family, Malware Hash MD5, Maware Hash SHA1, TTP) are expected in minimum in the IOC information to be provided	The details of IOC/IOA need to be comprehensive with the applicable Cyber Observables associated with respective attack.
99	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 17.The solution should be able to do Email security assessment (improper configuration or implementation of email filters)	The solutions should send real malicious emails to dedicated email accounts within the Bank to send threats, like malware and spear phishing links, and/or send sensitive information out of the bank's network to tests effectiveness of bank's email controls.	Bidder has to comply with the RFP terms.

D.I.T. Wing, Procurement
CANARA BANK
H.O., Bengaluru - 560 00

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
100	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 19.Endpoint Assessment - test security state of endpoints by comprehensively testing regardless of the method used to do the assessment. -	"Endpoint Assessment- The solution should have the ability to execute destructive attacks and behaviours in a safe endpoint environment to validate kill chain behaviour". ------------------------------ Note: (Destructive malware attack simulation at end user machine will help bank to gauge the efficacy of the endpoint security deployed in the bank 's end user machines, this performs in a safe environment)	Bidder has to comply with the RFP terms.
101	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 25. 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.	The solution should have the ability to execute destructive and non-destructive attacks safely in the bank's environment without spreading malware or infected files to other systems.	Bidder has to comply with the RFP terms.
102	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 26. 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.	The solution should have the ability to identify the exact response provided by security controls and validate them against measures such as block, detect, log, alert or missed and map how hosts interact with files, including malware, across endpoint environment. (eg: if the file transfer was blocked by firewall or if the file was quarantined by antivirus or detected by EDR)	Bidder has to comply with the RFP terms.
103	40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 28.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.	The solution should be able to generate detailed report covering the attacks which were successful and should have the detail of the TTP's and behaviors on how the attack played out in the environment (Attacker TTP's are more powerful than the IOC's)	Bidder has to comply with the RFP terms.
104	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 33. The solution should be capable of importing data from various sources like CMDB to do prioritization.	Prioritization of what ?, what type of Data ? Please define clearly various sources. Needs clarification and clarity. The clause should be solution should be allowed to import custom made payloads and run them on priority	Bidder has to comply with the RFP terms.
105	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 32. Determine which controls are most and least valuable; i.e., prioritization of controls.	This is kind of assets management. Why do we need this feature on bas solution ? May you remove it if possible?	Bidder has to comply with the RFP terms.
106	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 33. The solution should be capable of importing data from various sources like CMDB to do prioritization.	Simulation environment doesn't require a current customer asset.What is the use-case here? , Why do we need this feature?	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
107	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 29. The solution should have the capability to provide the Indication of Attack (IoA) based on the tool intelligence of detecting IOCs, behaviour, other contextual information etc. about the attacks.	Suggested clause: The solution should have the capability to provide the exact TTP based on platform intelligence and research and correlate it with industry standards such as MITRE ATT&CK, NIST, OWASP etc.	Bidder has to comply with the RFP terms.
108	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 30. 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.	Suggested clause: 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 and the mitigation steps has to be based on the correlation rules.	Bidder has to comply with the RFP terms.
109	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 31. The tool should be able to customise the risk categorisation. The report generated should highlight the attacks detected along with the category of the same ans risk associated with them.	Suggested clause: The solution platform should be able correlate results against attack vectors and quantify the effectiveness of the bank's security controls against defined risk objectives. Evidence should be produced by the solution to justify reasoning for risk and effectiveness scores along with evidence backed countermeasures.	Bidder has to comply with the RFP terms.
110	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 33 . The solution should be capable of importing data from various sources like CMDB to do prioritization.	Suggested clause: The solution should be capable of importing data from various sources including Bank's internal intelligence collection databases.	Bidder has to comply with the RFP terms.
111	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 29.The solution should have the capability to provide the Indication of Attack (IoA) based on the tool intelligence of detecting IOCs, behaviour, other contextual information etc. about the attacks.	Which all Cyber Observables (IP, Domain Name, CnC, Bitcoin Family, Malware Hash MD5, Maware Hash SHA1, TTP) are expected in minimum in the IOC information to be provided	Bidder has to comply with the RFP terms.
112	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 34.Continuously simulate breach methods to address changing risks, and track security posture via risk trending and historical reports.	Does Bank have any existing Automated Risk Assessment tool deployed for the NIST or any equivalent asset value and security posture awareness?	Bidder has to comply with the RFP terms.
113	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 35.Solution should integrate with the Security Operations Centre tools and judge the effectiveness of the same by simulating multi-vector attack.	Which SIEM tool is expected to be integrated with the Simulation Tool? Also, does it support REST API or Ansible?	The same will be shared with the selected bidder.
114	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 36.The solution support red team activities (attack scenarios) and blue team activities (actionable remediation).	Is the expectation for the Red Team with any specific Arsenal or Tools and for how many simultaneous consultants to run the simulation? Also is it expected to run one simulation use case at a time or multiple in Parallel	The decision will reside with the bank and would be provided to the selected bidder.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
115	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 29.The solution should have the capability to provide the indication of Attack (IoA) based on the tool intelligence of detecting IOCs, behaviour, other contextual information etc. about the attacks.	The solution should have the capability to provide the exact TTP based on platform intelligence and research and correlate it with industry standards such as MITRE ATT&CK, NIST, OWASP etc.	Bidder has to comply with the RFP terms.
116	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 30. 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.	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 and the mitigation steps has to be based on the correlation rules.	Bidder has to comply with the RFP terms.
117	41	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 31. The tool should be able to customise the risk categorisation. The report generated should highlight the attacks detected along with the category of the same ans risk associated with them.	The solution platform should be able correlate results against attack vectors and quantify the effectiveness of the bank's security controls against defined risk objectives. Evidence should be produced by the solution to justify reasoning for risk and effectiveness scores along with evidence backed countermeasures.	Bidder has to comply with the RFP terms.
118	41	Annexure-8	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 33. The solution should be capable of importing data from various sources like CMDB to do prioritization.	The solution should be capable of importing data from various sources including Bank's internal intelligence collection databases.	Bidder has to comply with the RFP terms.
119	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 42. The solution should not be dependent on other solutions for sourcing threat feeds.	This clause contradicts clause 9 (page No 39): 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. At one side you ask to source the threats and same time you say you should not be dependant on other source feeds. This clause needs to be removed.	The solution should have the capability to receive feed from multiple source and should not depend on any feed only from one source. Clause 9 doesn't pertain to forementioned.
120	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 44. Measure the time to detect and respond the attack simulation.	Needs clarication. Detection means, checking the attack results from the dashboard or something else ?	The solution should have the capability to compute the time to detect & respond to the detected attack.
121	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 46. 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.	Which systems should be supported ?	The detail will be provided to the selected bidder.
122	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 52. The solution should not add/create any performance degradation in the network.	We offer a new explanation to be on the safe side. "The solution should not add/create any performance degradation in the network and shouldn't send threats towards customer assets directly to aviod false positives"	Bidder has to comply with the RFP terms.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
123	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 43. The solution should be able to integrate with ticketing platforms.	We would request bank to remove this clause. As the proposed BAS solution is designed to simulate the attacks, hence ticketing platform integrations is not required.	Bidder has to comply with the RFP terms.
124	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 44 . Measure the time to detect and respond the attack simulation.	Suggested clause: The solution should be able to correlate results with observed SOC metrics as measured by the bank's Blue Team.	Bidder has to comply with the RFP terms.
125	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 47 . The solution should have the capability of providing attack blocking / prevention analysis.	Suggested clause: The solution should have evidence based capability of providing attack blocking/detection analysis.	Bidder has to comply with the RFP terms.
126	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 43. The solution should be able to integrate with ticketing platforms.	Does the Ticketing Platform support the API, XMl integration	The same will be shared with the selected bidder.
127	42	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 54.The solution should have the ability to execute complete attack library across network topology.	Please specify the Attacks library or libraries that is being referred in this specification, as it is difficult to openly claim that the support is available for complete Attacks library.	Bidder has to comply with the RFP terms.
128	42	Annexure-9	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 43. The solution should be able to integrate with ticketing platforms.	We would request bank to remove this clause. As the proposed BAS solution is designed to simulate the attacks, hence ticketing platform integrations is not required.	Bidder has to comply with the RFP terms.
129	42	Annexure-10	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 44. Measure the time to detect and respond the attack simulation.	The solution should be able to correlate results with observed SOC metrics as measured by the bank's Blue Team.	Bidder has to comply with the RFP terms.
130	42	Annexure-11	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 47. The solution should have the capability of providing attack blocking / prevention analysis.	The solution should have evidence based capability of providing attack blocking/detection analysis.	Bidder has to comply with the RFP terms.
131	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 57. The solution should have the capability of Auto discovering the security technologies deployed in the infrastructure including but not limited to SIEM, Proxy, IDS, Firewall, DLP, Endpoint Protection and malware analysis tools.	This clause defets the purpose of Breach attack Simulation technology. The attack should be executed without knowledge of any of defensive technology and configurations. Attack after having knowledge of secuirty Technologies is not a real attack. The best BA solution is that solution that does look at defensive solutions..This clause should be removed.	Bidder has to comply with the RFP terms.
132	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 64. Solution should be able to detect if the latest security patch are updated in the system.	Latest patch detection is job of Defenseive solution. Attack solution is to attack missing patches and exploit. Clause should be worded as solution should able to attack and exploit missing patches and launching multiple vector attack.	The solution should be able to perform attack by exploiting the missing patches and the report has to be generated highlighting the issues due to missing latest patches.

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

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
133	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 61. The solution should have the capability of providing Detect, Alerting analysis including SIEM Correlation rule analysis.	Which systems should be supported ?	The detail will be provided to the selected bidder.
134	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 64. Solution should be able to detect if the latest security patch are updated in the system.	This is a vulnerability centric approach.There are different tools to manage patching process. Can we remove this clause?	Bidder has to comply with the RFP terms.
135	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 64 . Solution should be able to detect if the latest security patch are updated in the system.	We would request bank to remove this clause as BAS platform cant determine the latest security patch are updated in the end user machine.	Bidder has to comply with the RFP terms.
136	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 65 . The solution should have the facility to integrate with the existing VA Tool of the bank to obtain information about existing vulnerabilities.	Suggested clause: The solution should be extensible to integrate TTP from external tools such as VA tool and cross-correlate attack results.	Bidder has to comply with the RFP terms.
137	43	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 65.The solution should have the facility to integrate with the existing VA Tool of the bank to obtain information about existing vulnerabilities.	Please specify the VA Tool in consideration for the support?	The same will be shared with the selected bidder.
138	43	Annexure-12	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 64. Solution should be able to detect if the latest security patch are updated in the system.	We would request bank to remove this clause as BAS platform cant determine the latest security patch are updated in the end user machine.	The solution should be able to perform attack by exploiting the missing patches and the report has to be generated highlighting the issues due to missing latest patches.
139	43	Annexure-13	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 65. The solution should have the facility to integrate with the existing VA Tool of the bank to obtain information about existing vulnerabilities.	The solution should be extensible to integrate TTP from external tools such as VA tool and cross-correlate attack results.	Bidder has to comply with the RFP terms.
140	44	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 68. The bidder should propose an on -premise solutions and no information should be sent outside the organisation, unless it has got dependency for testing any external testing component, with specific consent of the bank. Additionally the solution should have no dependency on the cloud for the on-prem deployment except for the updates, upgrades for the solution and security contents.	How can On premise solution simulate attack like Outside - In attack like Email, WAF, phishing ? Attack has to launched from outside, so some component of solution has to be outside. How can on premise solution simulate Data exfiltration attack ? Or any inside-out attack, To show a successful Attack sample data has to taken outside. This clause is contradictory to all clauses of Email, WED, DLP assessment. Clause should be worded as Solution should have On Prim and cloud component to carry out Inside out and outside In attack. And should ensure that No PII and SPDI data should leave bank.	The bidder should propose an on -premise solutions and no information should be sent outside the organisation, unless it has got dependency for testing any external testing component, with specific consent of the bank. Additionally the solution should have no dependency on the cloud for the on-prem deployment except for carrying out intended activity, the updates, upgrades for the solution and security contents.

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
141	44	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 69.The solution should be able to import samples of sensitive data from solution such as DLP.	Is it expected to take this information of samples from deployed DIP solution at Canara Bank or any DIP Solution.	The same will be shared with the selected bidder.
142	45	Annexure- 7 (A)	SI /Bidder Capability Questionnaire	Table 1: Questionnaire for Past Experience	These 5 references are of Only Bidder Or only of BAS player ? Or cumulative ?	Reference from the organisation where the solution has been deployed.
143	45	Annexure- 7 (A) SI /Bidder Capability Questionnaire	Table 1:	Questionnaire for Past Experience	This being relative new solution in the market Bidder does not have any reference. Hence request Bank to delete this clause	Bidder has to comply with the RFP terms.
144	46	Annexure- 7 (A) SI /Bidder Capability Questionnaire	Table 4:	Team Profile	This being relative new solution in the market Bidder does not have any reference. Hence request Bank to delete this clause	Bidder has to comply with the RFP terms.
145	47	Annexure- 7 (B)	SCORING MATRIX		This being relative new solution in the market Bidder does not have any reference. Hence request Bank to delete this clause	Bidder has to comply with the RFP terms.
146	57	Appendix -A	Instructions to be noted while preparing/submitting Part A- Conformity to Eligibility Criteria	15) Signed Pre Contract Integrity Pact as per Appendix-I on non-judicial Stamp paper.	Integrity Pact We agree to execute the Integrity Pact given by Canara Bank, provided that there is no Fall Clause in it. Please note that prices quoted are based on several factors, including quantity, location of delivery, dollar rates, discounts received from OEMs and other contractual risks. For all practical purposes, we request deletion of the Fall Clause from the Integrity Pact. We also wish to bring to your notice, that by way of Office Order dated 4/12/2007, the Central Vigilance Commission (CVC) even circulated copy of an Integrity Pact, drafted by SAIL and vetted by the Additional Solicitor General, for reference of individual organizations. The same does not contain any Fall Clause. Additionally, CVC issued a Circular dated 13.01.2017, formulating standard operating procedure for adoption of Integrity Pact and the same does not include Fall Clause as an essential ingredient of the Pact. Please refer to the enclosed Office Order and Circular, issued by the Central Vigilance Commission, for your information.	Bidder has to comply with the RFP terms.
147	19-21	C. DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	DELIVERABLES & SERVICE LEVEL AGREEMENTS (SLAS)	7. Support 9. Warranty 10. Annual Maintenance Contract (AMC) / Annual Technical Support (ATS) (if contracted) 11. Scope Involved During Warranty and ATS Period (if contracted) 12. Mean Time Between Failures (MTBF) 13. Subcontracting 14. Defect liability	Bank to kindly confirm that warranty, support, AMC/ATS conditions in respect of products/software supplied will be as per the OEM/OSD warranty terms and conditions and Bidder being an authorized reseller, will pass on such warranties "as-is", to the Bank."	Bidder has to comply with the RFP terms.

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

Prebid Queries Replies to RFP 13/2020-21 dated 02/09/2020 for Supply, Installation, Implementation, Roll Out, Operations and Maintenance of Breach Simulation Solution in Canara Bank.

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
148	38 & 40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 1. All installed agents/simulators should have capability to run assessments/simulations as local user privilege or admin user privilege. 2. The simulation agent should be compatible on various platforms like Window, Linux, MAC OS etc. 3. The solution should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations. 25. 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.	What is the total number of machines on which the simulator/agent needs to be installed?	The decision will reside with the bank and would be provided to the selected bidder.
149	38 & 40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 1. All installed agents/simulators should have capability to run assessments/simulations as local user privilege or admin user privilege. 2. The simulation agent should be compatible on various platforms like Window, Linux, MAC OS etc. 3. The solution should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations. 25. 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.	Please share the inputs on the versions of the Mac OS, and version with flavor of linux as this will help us arrive at the compliance as only Windows and Applications details are only given the Clause 4.1 on page 38	The assessment has to be undertaken on all the OS types & versions

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

Sl. No.	Page No.	Section	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
150	38 & 40	Annexure-7	Technical & Functional Requirement of Breach and Attack Simulation Solution	B. FUNCTIONAL REQUIREMENTS 1. All installed agents/simulators should have capability to run assessments/simulations as local user privilege or admin user privilege. 2. The simulation agent should be compatible on various platforms like Window, Linux, MAC OS etc. 3. The solution should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations. 25. 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.	Is it required on all the production desktops, laptops of the systems across Canara Bank including Zonal, Regional and Branch Offices or is it required in a Sanboxed Environ Machines	Bidder has to comply with the RFP terms.
151	NA	NA	NA	NA	There are no minimum specifications for Servers & Storage components.	Bidder has to specify the detail which is required for the implementation of the project.
152	NA	NA	Additional Query	NA	We would request bank that, Since it's a simulation tool the Verodin director (Main component) deployment is not required at both in DC & DR locations, deployment at one location will suffice with High availability enabled at director level.	Bidder has to comply with the RFP terms.
153	NA	NA	Additional Query	NA	We would require the sizing details from bank kindly review the attached spread sheet and fill the details accordingly, this information will help us in sizing the solutions. (Pls see the embedded excel files (2 files)within this document)	The detail will be provided with the selected bidder.
154	NA	NA	Additional Query	NA	We would require the below system requirement from the bank for the POC as well. (Page 25- Clause-4.2)	The same would be considered at the time of POC
155	NA	NA	Additional Query	NA	We would request bank that, Since it's a simulation tool the Verodin director (Main component) deployment is not required at both in DC & DR locations, deployment at one location will suffice with High availability enabled at director level.	Bidder has to comply with the RFP terms.
156	NA	NA	Additional Query	NA	Bank will not provide any remote sessions and direct internet connectivity to the equipment in terms of support which may leads to vulnerability.- (Page 14 /Clause 2.2) How will the TAC troubleshoot over remote in case of any technical issue arise. ?	Bidder has to comply with the RFP terms.
157	NA	NA	Additional Query	NA	Requirement Gathering Sheet and Requirement Questionnaire	The details will be provided with the selected bidder.

Place: Bengaluru
Date: 23/09/2020

Deputy General Manager

D.G.M., Wing, Procurement
CANARA BANK
H.O. Bengaluru - 560 001