


Sl No.	Page	RFP Clause	Our Requirements	Queries raised by the bidders	Reply By the Bank
1	5	Eligibility Criteria Point No 6	The proposed services should have been provided by the bidder to at least one Public Sector Bank/ Private Sector Bank in India in the last 2 years and the services must be currently running. For which, Letter from the Bank to be produced for having successfully implemented	The proposed services should have been provided by the bidder or OEM of the bidder to at least one public sector bank/ private sector bank in India in the last 2 years and the services must be currently running. We request the Bank to consider the "Customer Satisfaction Survey Reports" of other banks for similar services offered by us as it will give more details on satisfactory working of the solution. A mere implementation letter will fail to capture these important details in depth.	The clause is rephrased to read as "The proposed services should have been provided by the bidder to at least one Public Sector Bank/ Private Sector Bank in India in the last 2 years and the services must be currently running. For which, Letter to be produced by the bidder from the Bank to the effect that monitoring services are satisfactory".
2	11	1.13.1.J	Satisfactory working certificate from minimum 1 major clients as per Eligibility Criteria (4) for having implemented similar implementation of Anti-phishing, Anti-pharming, Anti-trojan, Anti-malware managed services	Same as above	The clause is rephrased as " The bidder should give an undertaking that the tools, architecture and details of Software used are adequate to run the managed services"
3	12	1.13.1.m	Manufacturer / Dealer / Distributor Certificate Certificate from OEM/ Manugacturer for proving 3 years experience.	- Does this imply that a) the OEM has to be in the business for the past 3 years? Or b) Does it demand proof for 3 years relation of the bidder with the OEM?	The clause is rephrased as "The bidder shall be the owner / certified or authorised agent / partner of the solution offered. Proof to be provided by Bidder in case he is not owner of the solution"
4	12	1.13.2 a	The Bidder also to submit a certificate / letter from OEM of the Application software that the proposed Architecture offered by the bidder to the Bank are relevant as no agent/client/device is going to implemented in correct, viable, technically feasible for bank's network as the all concerned Anti-fraud services would implementation and the solution will work without be internet cloud based. any hassles.	OEM Certificate supporting the bidder's implementation is not implemented in correct, viable, technically feasible for bank's network as the all concerned Anti-fraud services would implementation and the solution will work without be internet cloud based.	The bidder to comply with RFP terms
	12	1.13.2 e	A detailed list of the other Infrastructure hardware if any, required and any other precautions to be undertaken should be given in detail along with the Technical Bid.	A computer machine with SFTP clients and reporting application will be implemented only if referral logs monitoring is to be done and Web server will not send the referral logs directly to OEM.	The clause is rephrased to read as "A detailed list of the other Infrastructure hardware if any required at Bank's end and the precautions to be taken should be given in detail along with the Technical Bid "
5	16	2.6	Penalty: If the Selected Bidder fails to maintain response time (take down should happen within 4 hours from date and time of the anti phishing, anti pharming, anti malware scanning and anti Trojan incidents), penalty will be charged at the following rates- Response time for >8 hrs but <=12 hrs - 5% of quarterly payment Response time for >12 hrs but <=24 hrs - 10% of quarterly payment Response time exceeding 24 hrs - 24% of quarterly payment	Site take down is a Best of Effort basis activity. Site take down is a activity wherein there are multiple agencies involved in achieving the same. Bank is also a party to this along with Bidder, OEM and ISP. So it's difficult to sign an SLA for the site take down. so we request the bank to ease the SLA and put the clause as "Best of Effort Basis".	The clause is modified as follows: Penalty: If the Selected Bidder fails to maintain response time (take down should happen within 4 hours from date and time of the anti phishing, anti pharming, anti malware scanning and anti Trojan incidents), penalty will be charged at the following rates- Response time for >4 hrs but <=12 hrs - 5% of quarterly payment Response time for >12 hrs but <=24 hrs - 10% of quarterly payment Response time exceeding 24 hrs - 20% of quarterly payment Bidder to comply the above terms.

Sl No.	Page	RFP Clause	Our Requirements	Queries raised by the bidders	Reply By the Bank
6	18	2.11	Local Support: The Bidder should be capable of meeting the service & support standards as specified in this tender. Service support should be available on all Bank working days/ hours.	Local support is not relevant as no agent/client/device is going to implement in bank's network as the all concerned Anti-fraud services would be internet cloud based. If referral logs are transferred through a separate machine, the machine's SFTP & reporting application support will be taken care by SOC through IPSEC VPN, Desktop and OS support will be taken care by bank.	The bidder to Comply with RFP terms
7	22	3.7	Scope of Work: In case any account is compromised, proper tracking and reporting of fund is mandatory. The bidder has to assist the bank in case of legal case being raised by the customers for all such cases.	Accounts compromised? Does tracking of the same fall under scope of work? Tracking of the amount of fund transferred is not possible under anti phishing services. However the Bank has come up with the EOI for AA (Adaptive Authentication). The same benefit can be achieved using AA. Request the bank to ease this clause.	The bidder to Comply with RFP terms
8	23	3.24	In case of phishing and Pharming incidents, if the same incident becomes active on the same server within a period of 90 days of its previous closure, it should not be treated as a new incident.	Attack is same if active on same server within 90 days? The site take down is an activity which involves multiple agencies. 90 days is a too long time to consider since the OEM's consider calendar month as a bench mark to count the incidences. Request the bank to reduce the time period accordingly.	The bidder to Comply with RFP terms
9	36	6	Technical Specifications and Technical Evaluation Criteria: The bidder should have contacts/tie ups with major browser vendors, Internet Service Providers (ISPs) and other third parties to ensure faster closure of incidents. Should have tie ups with 1000+ ISPs in at least 50 countries.	All the ISP tie ups are normally attributable to the OEM. Request the Bank to rephrase the sentence to "The bidder should service the bank from an OEM who has to tie up with ..."	The clause is rephrased to read as "The bidder / OEM should have contacts / tie ups with major browser vendors, Internet Service Providers (ISPs) and other third parties to ensure faster closure of incidents. Should have tie-ups with 1000+ ISPs in atleast 50 countries
10	39	Technical Evaluation Part II	Parameters 1 to 10	The parameters 1 to 7 are OEM specific. Request the bank to use the parameters to rate the OEM a bidder ties up with & offers a solution to the bank. So request the bank to use parameters 1 to 7 to rate the OEM the bidder ties up with & the remaining parameters can be used to rate the bidder.	The Technical Evaluation Part II on Page 39 of 41 is modified as under - " The Table below contains a score of 100. A bidder/OEM of the bidder after complying with the requirements of Annexure - I ie., "Technical Specifications and Technical Evaluation Criteria" should also score minimum marks of 50 from this table ie., "Technical Evaluation part II."

Sl No.	Page	RFP Clause	Our Requirements	Queries raised by the bidders	Reply By the Bank
11	37	12	The bidder should have the capability to integrate these services into Security operation Centre (SOC) on real time.	<ol style="list-style-type: none"> 1. Is the bank looking for incident consolidation or integrate with SIEM? 2. Incidents would be generated and intimated to the bank... to a specific mail address(s) 3. SOC is more to monitor the banks infra and having this would not help. 4. Having a comprehensive incident handling for both internal [from SIEM or external from Anti-phishing, Trojan etc...] would help .. 	The bidder should have the capability to integrate the services on real time in case the bank decides to have SOC in future
12			General: Domains not mentioned	Request the bank to share the details of the domains to be monitored.	Domain site https://www.canarabank.in (Netbanking Site) Domain site https://www.canarabank.com (Corporate Site)

Place Bangalore
Date: 20.06.2011



 Deputy General Manager
