Pre-Bid Queries and Replies for RFP 19/2017-18 dated 07/11/2017 for Implementation of Anti-Phishing, Anti-Pharming, Anti-Malware, Anti-Trojan, Rogue attacks, Website defacement and Dark Web Monitoring managed services

Sl. No.	Page No.	RFP Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
1	8	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.1.** Visibility -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	As per the best practices, it is not advisable to continually monitor email as this may hamper performance. Request the bank to kindly clarify on the frequency of analysis and monitoring.	The Bidder can be provided DMARC reports and abuse Box from Bank's Mail Exchange Server.The bidder needs to have the capability of integration and should configure frequency of analysis and monitoring to detect the incidents within SLA. Bidder has to comply with RFP terms.
2	8	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.1.** Visibility -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	What is expected in DMARC reports	The Bidders can be provided with DMARC reports on periodic intervals and needs to block mail sent from Public exchange Servers like Google , yahoo etc. Bidder has to comply with RFP terms.
3	8	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.1.** Visibility -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	Abuse mail box monitoring service is not provided by Paladion. Can this be excluded from scope of work.	Abuse mail box includes mails phishing mails reported by customers and employees . The bidder needs to take up with mail service providers to block such phishing attempts. Bidder has to comply with RFP terms.

4	9	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.3.** Expedited Attack Takedown - Rapidly removal of identified threats before customers or employees become aware of a disruption.	General SLA for taking down a phishing site, fraudulent mobile Apps is 72 hours. Request the bank to consider to modify the SLA to 72 hours as complete takedown takes time depending on factors such as geography hosting, sector etc.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
5	9	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.5.** Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	It is not feasible to block the emails even before they reach the Canara Bank employees and customers. Request the bank to remove the RFP clause.	The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers. Bidder has to comply with RFP terms.

6	9	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.5.** Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Paladion shall not cover this scope. Can this be excluded from scope of work.	The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers. Bidder has to comply with RFP terms.
7	9	7. Scope of work:	**7.1.** The Bidder shall have the ability to perform the scope of work which includes the following: **7.1.5.** Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Prevention of Spoofing (or spoof emails coming pretending to come from Canara Bank's domain) requires implementation of software solutions like SPF and DMARC. Is bank looking for similar solution? In case this RFP is for Anti-Phishing, request bank to remove this point.	Implementation of SPF and DMARC is not in scope of the RFP.
8	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.1.** Solution must be a tool based automated solution with e-mail and SMS Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	Paladion shall provision service alerts via the portal and emails. Can this be excluded from scope of work.	SMS/Call should be done for high serverity incidents.

9	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.1.** Solution must be a tool based automated solution with e-mail and SMS Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	Solution proposed by RSA will send such alerts on e-mail and 24x7 online dashboard.	SMS/ call should be done for high serverity incidents.
10	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.4.** Solution must support scanning of static and dynamic links.	What depth are being referred here ? Kindly clarify	Depth refers to the corresponding pages available in a domain.
11	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.4.** Solution must support scanning of static and dynamic links.	What depth are being referred here ? Kindly clarify	Depth refers to the corresponding pages available in a domain.
12	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.4.** Solution must support scanning of static and dynamic links.	What depth are being referred here? Kindly clarify.	Depth refers to the corresponding pages available in a domain.
13	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.1.** Solution must be a tool based automated solution with e-mail and SMS Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	Request you to modify this clause to -. olution must be tool based automated solution with email and/or SMS alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web	SMS/ call should be done for high serverity incidents.
14	8	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.1.** Solution must be a tool based automated solution with e-mail and SMS Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	Solution proposed by RSA will send such alerts on e-mail and 24*7 online dashboard.	SMS/ call should be done for high serverity incidents.

15	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.2.** 24*7*365 real time monitoring and support for all the services covered under the scope of this RFP.	24*7*365 real time monitoring requires deployment of Full Time resources at the Bank's premises. Kindly confirm if this is the expectation of the Bank.	The Bidder has to provide real time monitoring and support for all the services covered under the scope from it's SOC Centre.
16	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.3.** Solution must support scanning to a depth of multiple pages.	This is part of Antimalware Service and does not fall under Ant phishing Service	Even though Scanning is being done as part of malware service , anti phishing detection should also be done on all the pages within the domain. Bidder has to comply with RFP terms.
17	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.4.** Solution must support scanning of static and dynamic links.	This is part of Antimalware Service and does not fall under Ant phishing Service	Even though Scanning is being done as part of malware service , anti phishing detection should also be done on all the pages within the domain. Bidder has to comply with RFP terms.
18	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.5.** Solution must support checking all website links against well-known global black list.	This is part of Antimalware Service and does not fall under Ant phishing Service	Bidder has to comply with RFP terms.
19	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.6.** Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	Scanning of external applications for MMC infection is not feasible. Kindly clarify the expectation of the solution in terms of managing MMC code infections.	Bidder has to comply with RFP terms.
20	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.6.** Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	This is part of Antimalware Service and does not fall under Ant phishing Service	Bidder has to comply with RFP terms.

21	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.12.** Solution should provide for identification of fake recruitment schemes claiming affiliation with the bank.	These fake schemes will be detected only if any third party website is infringing on Canara Bank copyright.	Identifying of fake recruitment schemes using Canara Bank's name , logo etc should be informed to the Bank.
22	9	7. Scope of work:	**7.2.** Solution should have following features but not limited to: **7.2.16.** Vendor should assist the Bank in forensic investigation for in scope domains and mobile apps.	What exactly is required - Forensic Investigation, Incident Analysis or Cyber Cell Response? How many no. of hours of Investigation we should factor? Is Bank open to pay on consume-as-we-go?	Forensic analysis or investigation won't be entrusted to the bidder . The bidder needs to support the Bank for details requested on In-scope services.
23	10	7. Scope of work:	**7.3.** Early Phishing Detection: **7.3.4.** Implementation of watermark and other means/techniques for each website.	Request the bank to further clarify on the requirement. Watermark for external sites not possible.	Bidder has to comply with RFP terms.
24	10	7. Scope of work:	**7.3.** Early Phishing Detection: **7.3.8.** Provide need based analysis on suspicious e-mail messages.	This is not a part of standard deliverable. However, it can be considered as an ad-hoc activity. 5 email/month can be analysed. Please confirm	Since analysis on suspicious mails will be requested only on the In-scope services, the clause remains the same as in RFP. Bidder has to comlply with RFP terms.
25	10	7. Scope of work:	**7.3.** Early Phishing Detection: **7.3.10.** Should have mechanism to call, mail or send sms to Bank on the basis of severity of incident.	Paladion shall provision service alerts via the portal and emails. SMS is not part of the mode of communication.	SMS/ call should be done for high serverity incidents.

26	10	7. Scope of work:	**7.5.** Email Fraud Protection : **7.5.1.** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	This is not a part of standard deliverable and also Paladion does not cover the same. Can this be removed scope of work.	The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers. Bidder has to comply with RFP terms.
27	9	7. Scope of work:	**7.5.** Email Fraud Protection : **7.5.1.** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	Our OEM partner doesn't provide takedown SLA as it is dependent on multiple factors depending upon the incident type. However, we can guarantee the blocking of the attack thru browser partnerships.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
28	10	7. Scope of work:	**7.5.** Email Fraud Protection : **7.5.1.** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	We understand by Email Fraud protection, expectation is to monitor abuse mail box and identify potential threats. Please confirm.	The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers .

29	10	7. Scope of work:	**7.5.** Email Fraud Protection : **7.5.1.** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	There are specific DAMRC solutions available to prevent e-mail frauds. However, RSA anti-fraud services can integrate with such solution providers as well conduct abuse mailbox monitoring to enhance phishing detection.	The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers .
30	10	7. Scope of work:	**7.5.** Email Fraud Protection : **7.5.1.** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	In order to have visibility across all emails send within the organization, email scanning solutions needs to be implemented. Please suggest if scanning of emails is in scope of this RFP, else request bank to remove this clause	Email scanning solution for Banks Mail exchange server is not in scope of the RFP . The scope covers detection and blocking of Fraud / Phishing mails coming to Bank Employees and customers from Public Mail exchange servers such as Google, Yahoo etc. Further Abuse Mail Box and DMARC reports will be provided to the bidder for detection of phishing / spoof mails sent to employees. The same needs to be blocked in Public Mail Exchange Servers. Bidder has to comply with RFP terms.
31	10	7. Scope of work:	**7.6.** Rogue Mobile Application Protection: **7.6.4.** Inject fake credentials into the phishing portals and fraudulent apps and provide details to the Bank for monitoring and blocking at Bank's end.	Request the bank to further clarify on the requirement.	Bidder has to comply with RFP terms.

32	10	7. Scope of work:	**7.7.** Dark Web/Deep Web Scanning for sensitive information pertaining to Bank: **7.7.4.** Maintain or have direct access to data from honey pots or network or sensors to collect data on threat.	Request the bank to kindly provide clarification on the requirement.	As per RFP
33	11	7. Scope of work:	**7.8.** Web Site/Web app related Monitoring: **7.8.4.** Blocking of the phishing sites in web browsers. The bidder needs to have tie-ups with Browser providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.	It is not feasible to have tie-ups with browsers providers. Request the bank to kindly remove the RFP clause.	Bidder has to comply with RFP terms.
34	11	7. Scope of work:	**7.8.** Web Site/Web app related Monitoring: **7.8.6.** The successful bidder should identify defacement of Bank website and corresponding WebPages through a combination of automated scans and manual analysis. **7.8.7.** The analysis should be done in a manner that only genuine defacements are informed to Bank and false positives are minimized.	Request the Bank to kindly consider keeping Anti-Defacement out of the scope of this RFP.	As per RFP
35	11	7. Scope of work:	**7.9.** Other Services: **7.9.2.** Assistance to the bank for coordination with law enforcement agencies, CERT-In etc.	We assume the support shall be limited to working with the bank employees and within the scope of the SOW. Kindly clarify.	The bidder needs to provide assistance to the Bank. The correspondence in such case will be with the Bank and not directly with the agencies.
36	11	7. Scope of work:	**7.9.** Other Services: **7.9.3.** Bidder must have capability of 24x7 real monitoring and detection for malicious mobile code (MMC) infection of Bank's websites and mobile applications.	Malware Scanning is 24/7 monitoring service, and scanning will be done at equal interval of 30 minutes as per industry best practises. Please confirm if this inline with the RFP requirement.	Bidder has to comply with RFP terms.

37	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to.	RSA doesn't provide takedown SLA as it is dependent on multiple factors depending upon the incident type. However, we can guarantee the blocking of the attack thru browser partnerships.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
38	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to:	Our OEM partner doesn't provide takedown SLA as it is dependent on multiple factors depending upon the incident type. However, we can guarantee the blocking of the attack thru browser partnerships.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
39	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.3.** Initial response to the incident within 30 minutes with action plan on taking down and other alternative response mechanisms.	It is feasible to intimate regarding the incidents to the Bank within first 30 minutes. Formulating the initial response plan requires discussion with the stakeholders from the bank. Kindly confirm if this is the expectation from the bank.	Initial response includes formulating the initial response plan and discussion with the stakeholders for future course of action.

40	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.4.** Take down of Phishing Site, fraudulent mobile apps within 8 hours of incident.	General SLA for taking down a phishing site, fraudulent mobile Apps is 72 hours. Request the bank to consider to change the SLA to 72 hours as complete takedown takes time depending on factors such as geography hosting, sector etc.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
41	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.4.** Take down of Phishing Site, fraudulent mobile apps within 8 hours of incident.	Taking down of sites involves lot of co-ordination with multiple agencies located in different GEO / Time Zones. Would there fore equest you to modify the clause as follows - SLA - Take down of phishing site, fraudulant mobile apps within 24 hours of incient.	The Phishing site should be blocked within 4 hours. The SLA for takedown of phishing site given in scope should be adhered to 90% of the takedowns per quarter. The remaining 10% takedowns per quarter should be completed within 72 hours of the incident but the phishing site should be blocked in all major browsers as per SLA.
42	13	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.7.** Resolution of Trojan incidents with 24 hrs of detection.	Request the bank to kindly clarify on what is the expected resolution of Trojan Incidents within 12 hours.	As part of resolution ,the bidder needs initiate an action plan with Bank and coordinate for closure of the event.
43	12	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.8.** In case of defacement of Bank's website and corresponding web pages, the bidder should alert Bank over call in 15 minutes.	Please share the no. of web pages under scope along with the no. of URLs	35 URLs , the web pages under each domain will be shared with successful bidder.
44	13	Annexure 1 Checklist point no. 5	Whether Escalation matrix, Preventive and Break down/ Corrective Maintenance is provided?	Paladion wish to understand the expectation in "Preventive and break down/Corrective Maintenance"	The clause refers to escalation matrix for incident response and communication with SOC team

45	14	7. Scope of work:	**7.12.** Followings are the important terms of SLA but not limited to: **7.12.8.** In case of defacement of Bank's website and corresponding web pages, the bidder should alert Bank over call in 15 minutes.	Request the Bank to kindly consider taking Anti-Defacement out of the scope of this RFP.	Bidder has to comply with RFP terms.
46	16	12. Preparation of Bids:	**12.4.** Technical Bid Evaluation Criteria	Getting work order / PO from customers will be a challenge for OEM. We would request you to modify this to accept OEM / Bidder Undertaking or Case studies as reference document.	Bidder has to comply with RFP terms.
47	16	12. Preparation of Bids:	**12.4.** Technical Bid Evaluation Criteria **7.** The Bidder/OEM has ISO 27001 Certified Security Operations Centre.	Marks related to SOC is not relevant to this bid. Pls delete.	Bidder has to comply with RFP terms.
48	16	12. Preparation of Bids:	**12.4.** Technical Bid Evaluation Criteria **7.** The Bidder/OEM has ISO 27001 Certified Security Operations Centre.	Marks related to SOC is not relevant to this bid. Pls delete.	Bidder has to comply with RFP terms.
49	16	12. Preparation of Bids:	**12.4.** Technical Bid Evaluation Criteria **7.** The Bidder/OEM has ISO 27001 Certified Security Operations Centre.	Customer data will not be handled in the SOC in any form. This is purely a scanning service of scanning the external cyber world to identify the potential attacks on customer. Therefore, ISO 27001 will not be relevant as bank will not share any operational data with the bidder/OEM. Request Bank to remove the requirement of ISO 27001 certification	Bidder has to comply with RFP terms.

50	29	44. Liquidated Damages: 44.2. Penalties/Liquidated damages for each Incident happened and not reported:	44.2.2. The maximum penalty levied shall not be more than the 20% (Plus GST) of total order value payable for that Year.	Request bank to cap the maximum penalty at 10% of the total order value for a year	The RFP clause is modified as under: "44.2.2. The maximum penalty levied shall not be more than the 10% (Plus GST) of basic invoice value."
51	30	44. Liquidated Damages:	44.3. Failure to resolve incidences like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents):	1. We understand that Resolution means that permanent / work around solution to protect users from further breaches / incidents. Please confirm. 2. Also, taking down sites involves co-ordination with multiple agences in different time zones. Request you to provide minimum 24 hour window to resolve incidents.	1. The clause mentions resolving of incident. Resolving here means interm measures to block access of phishing sites to user as per SLA in this clause followed by final measures such as take down. 2. The SLA given in scope for Takedowns should be adhered to 90% of the takedowns . The remaining 10% takedowns should be completed within 72 hours of the incident.
52	43	Annexure-3 Eligibility Criteria Declaration Criteria No. d	Eligibility Criteria: Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. Documents to be submitted: Certificate from customers to be produced	Is client expecting Masked PO copies of our customer	**Eligibility Criteria is modified as under:** "d. Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. **Documents to be submitted:** The Bidders must produce PO/Reference letter in their name from customers."

53	43	Annexure-3 Eligibility Criteria Declaration Criteria No. d	Eligibility Criteria: Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. Documents to be submitted: Certificate from customers to be produced	The requirement in the RFP is a set of service(s) provided by bidder/OEM. Experience of bidder or OEM should both be considered in the response. Specifically for services where bidder is engaging with a backend OEM, the experience of the OEM should be considered. We would request bank to modify same to bidder/OEM	**Eligibility Criteria is modified as under:** "d. Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. **Documents to be submitted:** The Bidders must produce PO/Reference letter in their name from customers."
54	43	Annexure-3 Eligibility Criteria Declaration Criteria No. d	Eligibility Criteria: Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. Documents to be submitted: Certificate from customers to be produced	Kindly change to OEM/bidder must have 3 years of experience in the field of implementation & monitoring of Information security business since services will be delivered by OEM & SI.	**Eligibility Criteria is modified as under:** "d. Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. **Documents to be submitted:** The Bidders must produce PO/Reference letter in their name from customers."
55	43	Annexure-3 Eligibility Criteria Declaration Criteria No. d	Eligibility Criteria: Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. Documents to be submitted: Certificate from customers to be produced	Request the bank to kindly clarify alternate documents acceptable to the bank in case it becomes difficult for the bidders to procure certificates from the customers in such a short span of time.	**Eligibility Criteria is modified as under:** "d. Bidder must have 3 years experience in the field of implementation and monitoring of Information Security Business. **Documents to be submitted:** The Bidders must produce PO/Reference letter in their name from customers."

56	43	Annexure-3 Eligibility Criteria Declaration Criteria No. e	Eligibility Criteria: The solution proposed by the bidder for services should have been provided by the Bidder to at least one Scheduled Commercial Bank in India in the last 2 years and the services must be currently running. Documents to be submitted: Letter from the Bank to be produced for having successfully implemented.	Request the bank to kindly consider relaxing the eligibility clause as the services quoted in the RFP are in early stage of adoption by the Banks in India. The solution proposed by the bidder for similar services should have been provided by the Bidder to atleast one Scheduled Commercial Bank/Financial Institution/ Public/ Private organizations in India or globally in the last 2 years.	Bidder has to comply with RFP terms.
57	43	Annexure-3 Eligibility Criteria Declaration Criteria No. f	Eligibility Criteria: Bidder should have minimum 5 CISA / CISM/ CISSP/ CIHE/ CVA/ CEH security related certification holders in the organization. Documents to be submitted: Profile of employees with certified copies.	Kindly change to OEM/bidder should have minimum 5 CISA/CISM/CISSP/CIHE/CVA/Ceh since service will be jointly delivered by OEM & SI.	Bidder has to comply with RFP terms.
58	51	Annexure-9 Technical Bid Covering Letter point no. g	Details of inputs/requirements required by the Bidder to execute this assignment.	**Kindly share -** 1. web & mobile app URLs under scope for Anti-phishing services, brand monitoring, 2. no. of web pages for web defacement 3. No. of URLs for anti-malware services	No. of URLs is: 35 No. of Mobile Apps is: 7
59	51	Annexure-9 Technical Bid Covering Letter point no. h	Conformity to the obtaining of various certificates/bench mark testing standards for the items quoted to meet the intent of the RFP	Paladion wish to understand client's expectation more in detail	Bidder has to provide confirmity to the RFP term.

60	51	Annexure-9 Technical Bid Covering Letter point no. j	Bidder is engaged in conducting Information Security Audit since (month & year) & total experience (in years/months) in Audit Services.	Is the Bank expecting duration for provision of Brand Monitoring & Anti-phishing services here?	Bidder has to mention number of years they are involved in providing Information Security Services.
61	55	Annexure-12 Undertaking Letter Format point f	f. We hereby undertake to provide necessary hardware with latest product and software with latest version and any third party licenses with latest version required for the implementation of the Services. The charges for the above have been factored in Bill of Material (BOM) or will be quoted in the Reverse Auction, otherwise the Bid is liable for rejection. We also confirm that we have not changed the format of BOM.	Anti-phishing services are online services and does not require any hardware provisions/arrangements to make, hence request client to kindly reframe the clause that is applicable to the anti-phishing & brand monitoring services only	Bidder has to provide confirmity to the RFP term.
62	58	Annexure 15	**Commercial Bid**	RSA Commercials are not based on no. of websites/domain names or mobile apps. RSA provides unlimited monitoring of banks domain names or apps. However, the pricing is only based on No. of takedowns subscription per year. Hence, Table B & C is not applicable, we would request bank to kindly delete the same. We also recommend to increase the no of takedowns to atleast 50 per year from current 25 mentioned in the RFP.	Amended Bill of Material is attached as Annexure.

63	58	Annexure 15	Commercial Bid	Majority of OEM / Service provider Commercials are not based on no. of websites/domain names or mobile apps Prices are based on no of take downs in an year. .. We also recommend to increase the no of takedowns to atleast 50 per year from current 25 mentioned in the RFP.	Amended Bill of Material is attached as Annexure.
64	58	Annexure 15	Commercial Bid	Our OEM is is a leading security OEM in the world. Their Commercials are not based on no. of websites/domain names or mobile apps. They provides unlimited monitoring of banks domain names or apps. However, the pricing is only based on No. of takedowns subscription per year. Hence, Table B & C is not applicable, we would request bank to kindly delete the same. We also recommend to increase the no of takedowns to atleast 50 per year from current 25 mentioned in the RFP as we observe from other similar sized banks & BFSI institutions.	Amended Bill of Material is attached as Annexure.
65	58	Annexure 15	Commercial Bid	Please specify the total number of URLs required to be scanned for Anti-Malware & defacement service.	Amended Bill of Material is attached as Annexure.

66	NA	NA	Anti-Pharming	Kindly clarify the scope for Anti-Pharming.	As per RFP

Deputy General Manager