RFP: KaGB: Project office: RFP: 01:2021/22 Dated : 23.06.2021					
Sr. No.	**Section & Clause Ref. No./Appendix no/Annexure no**	**Page No.**	**RFP text**	**Query**	**Response to Query**
1	6. Detailed Scope of work/6.20.1	11	Alert within 30 minutes of attack/compromise.	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Not a Valid Query
2	6. Detailed Scope of work/6.20.3	12	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 sit should be blocked in all major browsers as per SLA.	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
3	6. Detailed Scope of work/6.20.5	12	Resolution of Trojan incidents with in 24hrs of detection.	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
4	Penalty 19.3	15	Penalty for each Incident happened and not reported	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
5	Penalty 19.4	16	Penalty for failure to resolve incidences (to be calculated on quarterly average basis)	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
6	Penalty 19.5	17	Penalty for failure to resolve Trojan Malware incidents (To be calculated on incident basis)	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
7	Penalty 19.5	17	Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	It's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
8	20. Payment Terms	20.1	Payment shall be released Quarterly in Arrears at actuals	Request Bank to Amend Payment terms as Half Yearly Advance .	Bidder to comply with RFP terms
9	Annexure 01 - Eligibility Criteria Sl No 12	55	The services proposed by the Bidder/ the OEM should have been provided in at least One Scheduled Bank in India with minimum of 500branches during the last three years and the services must be currently running.	Kindly change this clause to "Relaxation to Make in India' product and MSME along with startup, for exemption from this criteria	Bidder to comply with RFP terms
10	6. Detailed Scope of work/6.20.1	11	Alert within 30 minutes of attack/compromise.	The time of attack is often unknown. How do we define start of attack? When spam is sent? Phishing site hosted? Hence, it's difficult to provide SLA since blocking and shutdown purely depends on the hosting partner such as google, godaddy etc. Requesting bank to get this clause removed	Bidder to comply with RFP terms
11	19.3.2	15	If the bidder fails to report incident like Phishing, Pharming, Brand abuse, Trojan, Malware, Website defacement (To be calculated for each and every incident) that has occurred and not reported to the Bank, penalty would be as under	Placing a timed parameter into a missed detection SLA is problematic.Requesting bank to get this clause removed.	Bidder to comply with RFP terms
12	19.4	16	Penalty for failure to resolve incidences (to be calculated on quarterly average basis)	Please revise SLA and calculate performance with MEDIAN time. We cannot accept AVERAGE time. Average time can be statistically skewed by outliers. Example - 95% of incidents are resolved in less then 2 hours. (An unrealistically good outcome), with 5% problematic cases that are unresolvable/uptime of days, Average will be skewed to outside of SLA parameters. MEDIAN is a more statistical meaningful calculation to employ.	Bidder to comply with RFP terms
13	19.6	17	Penalty for failure to resolve Trojan Malware incidents (To be calculated on incident basis)	Making this penality on per missed detection case is not acceptable. Vendor could provide a 99% detection (an unrealistically good outcome) and still fail the SLAs. Detection rate should be a percentage. Also - "prior to bank detecting/ any other party/ agency" - the bank could employ a competiting product - two equal vendors would only achieve a 50% detection rate with all parameters being equal. Remove this statement. "Maximum cap for penalty is 10% of Quarterly Payment of Darknet/ Deepweb Scanning Services" - potential 40% financial penality of total contract at risk is not acceptable.	Bidder to comply with RFP terms
14	19.5	17	Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	Please revise SLA and calculate performance with MEDIAN time. We cannot accept AVERAGE time. Average time can be statistically skewed by outliers. Example - 95% of incidents are resolved in less then 2 hours. (An unrealistically good outcome), with 5% problematic cases that are unresolvable/uptime of days, Average will be skewed to outside of SLA parameters. MEDIAN is a more statistical meaningful calculation to employ.	Bidder to comply with RFP terms
15	19.8	18	Penalty for failure to maintain response time for scanning of Banks website for defacement (to be calculated on incident basis)	One missed web defacement detection - equal 100% penality - this cluase is not acceptable. Requesting bank to get this clause removed	Bidder to comply with RFP terms
16	19.9	18	Also, bank will reserve the right to get such incidents closed from other parties, expenses for which shall be recovered from the vendor.	Not acceptable clause - costs are unknown / undefined. Requesting bank to get this clause removed	Bidder to comply with RFP terms
17	19.15	19	Maximum deducted penalty of one type will not affect any other type of penalty i.e. All type of penalties can be levied up to their maximum limit simultaneously.	Total penalities at risk equals more than the value of the contract. This Cluase is not acceptable clause. Requesting bank to get this clause removed.	Bidder to comply with RFP terms
18	20.1	19	Payment shall be released quarterly in arrears at actuals	Requesting bank to change the billing to be annual	Bidder to comply with RFP terms
19	Anneuxure 2 /4	56	The services is required to be provided with comprehensive scanning of URLs/Websites and provide report in various possible ways	The reports are not customizable.The reports are provided as scan report with recommendation, URL report,Content change report,security audit report , scan summary report.	Bidder to comply with RFP terms
20	Anneuxure 2 /5	56	Bidder must provide solution for 24X7 monitoring for Malicious Mobile Code (MMC) infection of the websites i.e. 24x7x365 monitoring / scanning of internet facing web applications of the Bank for real time detection of malware injection.	MMC injection detection is not supported, Malware scanning of internet facing web applications can be done as per the frequency. Minimum scan frequency can be of 6hrs.	Bidder to comply with RFP terms

21	Anneuxure 2 /8	56	Monthly and other ad-hoc reports to be provided as per the requirement and format provided by the Bank.	The reports are not customizable.The reports are provided as scan report with recommendation, security audit report , scan summary report. For security audit and scan summary user can apply datewise,domain wise filters etc.	Bidder to comply with RFP terms
22	Anneuxure 2 /10	56	Website domain tracking analysis to detect phishing sites.	Phising detection includes finding similar looking domains only, client has to verify from their side wether they are phishing sites or their own.	Bidder to comply with RFP terms
23	Anneuxure 2 /13	56	The vendor should have the ability to identify defacement of Bank website and corresponding WebPages through a combination of automated scans and manual analysis.	The Tools is completely automated , it will scan for defacement. No mannual analysis is performed.	Post scanning, the scan report could be analysed manually
24	Annexure 2 (Sub Section C)	57	3 Implementation of real time detection mechanisms and alerts. 4 Implementation of watermark and other means/techniques for each website. 5 Performing the services for detecting anti - phishing mechanisms such as referrer logs, watermarks etc. 6 Track hosting of phishing sites through implementation of watermark and other Means.		Not a Valid Query
25	Annexure 2 (Sub Section C)	57	8 Provide need based analysis on suspicious e-mail messages. 9 Monitoring spam traps to detect phishing mails 10 Should have mechanism to call, mail and send sms to Bank on the basis of severity of incident.	As per us the below point is not under the scope of our service , as we operate from external side,and we don't control you antispam on email,email spam is not domain. It has to be under thescope of Email service provider.	Refer to Amendment 01
26	20.9.14 Right to alter the number of websites and apps:	20	The Bank reserves the right to alter the number of websites and apps specified in the tender intheevent of changes in plans of the Bank. Any decision of the BANK in this regard shall befinal,conclusive and binding on the bidder. The bank reserves the right to place order for theseadditional numbers of websites and apps at the agreed price during the contract period with thesame terms and conditions	This has to be defined on day one as it cannot be open ended . We are taking it as 20URLs and 20 IPs as the base service requirements. Please clarify	Bidder to comply with RFP terms
27	18. Project Implementation Timeline	14	Configuration and Full implementation of all services Within 6 weeks from date of acceptance of PO	Request Bank to consider the current Pandamic situation and increase the timeline to 10 -12 weeks	Bidder to comply with RFP terms
28	NA	NA	NA	Anti Phishing, Brand and Dark web monitoring solutions/platforms operate outside the customer premise and monitor internet/public infrastructure only hence would be deployed in Cloud. Cloud deployment along with SaaS delivery model advised.	Not a Valid Query
29	6. Detailed Scope of Work - Sub section 6.1	9	Commissioning of services for 24X7X365 proactive Monitoring and Management of Bank's designated websites in World Wide Web for Anti-Phishing, Anti-Malware, Anti-Pharming, Anti-Web Defacement, Anti-Trojan, Rogue Attacks and Dark Web Scanning and any other threat or exploitation of vulnerabilities which lead to compromising of credentials of the customers unknowingly directed against the customers of the Bank. The Bank should get alerts in the event of above attacks on real time basis.	Request Bank to remove this clause	Bidder to comply with RFP terms
30	6. Detailed Scope of Work - Sub section 6.2	9	The selected bidder should respond immediately upon detection of any of the above attacks and should work to shut down/take-down the detected site, anywhere in the world also within the minimum possible time as specified in SLA on Real-Time Basis. For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers etc.	Request below amendments for clarity in scope and further delivery: "The selected bidder should respond immediately upon detection of any of the above attacks and should work to shut down/take-down the detected site, anywhere in the world also within the minimum possible time as specified in SLA. For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers/ Signature Approach/ Logo Matching etc. without compromising the detection of phishing sites"	Bidder to comply with RFP terms
31	6. Detailed Scope of Work - Sub section 6.7	10	Reporting to Bank in line with regulatory requirements about all the attacks and providing detailed information through email, dashboard, SMS alerts, phone calls etc. Details of compromised accounts should be shared immediately with the Bank. Conference call facility with the vendor team should available to bank in case requirement arises.	Request bank to remove SMS alert scope. However, Slack and WhatsApp group could be leveraged for urgent communication.	Bidder to comply with RFP terms
32	6. Detailed Scope of Work - Sub section 6.8	10	Take up and coordinate the cases with CERTs and / or other legal agencies as per the format provided by the Bank.	CloudSEK would be able to assist client for coordination with law enforcement agencies like CERT /or other legal agencies as per the format provided by the Bank on special requests and as per mutually decided timelines only	Would be called out by the Bank for the requiste incidents
33	6. Detailed Scope of Work - Sub section 6.9	10	Monthly and other ad-hoc reports to be provided as per the requirement and format provided by the Bank.	All the reports are automated and can be scheduled in the platform either Daily/Weekly/Monthly.	Ok with Bank as long as the requirement is met
34	6. Detailed Scope of Work - Sub section 6.10	10	Vendor will be required to submit monthly analysis and fraud intelligence reports (both high level/summarized and low level/detailed) to bank.	All the reports are automated and can be scheduled in the platform either Daily/Weekly/Monthly.	Ok with Bank as long as the requirement is met
35	6. Detailed Scope of Work - Sub section 6.14	11	Bank can also increase or decrease the scope of services during the period of contract with a notice of 30 days. Bank can increase or decrease the scope of services availed as per the RFP-BoM during the period of contract. If any new services are added to the scope, the same will be on mutually agreed basis.	Increase in scope would have an implication in the overall pricing and would be conveyed to KaGB and agreed by KaGB.	Refer to Amendment 01

36	6. Detailed Scope of Work - Sub section 6.15	11	The detailed list of Bank 's websites & mobile apps will be provided to successful bidder. However, this list is subject to change. Bidder will be required to monitor all the domains of the Bank including new domains Bank may acquire during the period of contract. Additional Websites or Mobile Applications to be included immediately for Monitoring and Managed Services on receipt of official communication from Bank. Bidder has to monitor the domains of the Amalgamated entity, if any, during the period of contract	Increase in scope would have an implication in the overall pricing and would be conveyed to KaGB and agreed by KaGB.	Bidder to comply with RFP terms
37	6. Detailed Scope of Work - Sub section 6.20 - Sub Section 6.20.1	10	Alert within 30 minutes of attack/compromise.	Our solution would report Alert within 30 minutes of attack/compromise from the sources it monitors. Request Bank to confirm if this is inline with Bank's requirement	Yes , Alert should be provided within 30 minutes of attack/compromise.
38	6. Detailed Scope of Work - Sub section 6.20 - Sub Section 6.20.3	11	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.	Phishing site blocking and takedowns are different. CloudSEK offers takedowns for phishing sites which is a preferred by Major banks and BFSI clients. As per the penalty, below would be advised. Maximum 15 takedown violations are accepted in a quarter. For every single violation after that, penalty will be charged 5% of per takedown price, Penalty Payment up to maximum 5% of overall takedown price per quarter in form of service extension.	Bidder to comply with RFP terms
39	6. Detailed Scope of Work - Sub section 6.20 - Sub Section 6.20.5	11	Resolution of Trojan incidents with in 24hrs of detection.	Request Bank to remove this clause	Bidder to comply with RFP terms
40	6. Detailed Scope of Work - Sub section 6.20 - Sub Section 6.20.6	11	In case of defacement of Bank's websites and corresponding web pages, the bidder should alert Bank over call/mail within 30 minutes.	Request Bank to remove this clause	Bidder to comply with RFP terms
41	6. Detailed Scope of Work - Sub section 6.20 - Sub Section 6.20.7	11	The bidder needs to monitor for sensitive data on Dark/Deep web and inform the Bank immediately for sensitive data available in dark web. The bidder also needs to submit bi-weekly/weekly reports on the incidents of data compromise detected on Dark web.	All the reports are automated and can be scheduled in the platform either Daily/Weekly/Monthly.	Ok with Bank as long as the requirement is met
42	17 Technical considerations for the RFP	14	Both Banks together are having approximately 14 websites and Mobile applications used in various applications developed/procured by the Bank. They are hosted on domains such as karnatakagraminbank.com, keralagbank.com, canarabankrrb.com, canbankrrb.com etc.	Please share all the top level domains name e.g. karnatakagraminbank.com, keralagbank.com, canarabankrrb.com, canbankrrb.com and remaining, that would need to be monitored on a continuous basis for KaGB. This would be critical for estimation purpose.	Would be Provided to Successful Bidder
43	19.1 Uptime	15	The bidder shall guarantee the availability of Monitoring and Managed Services towards Anti-Phishing, Anti-Malware, Anti-Pharming, Anti-Web Defacement, Anti-Trojan, Rogue Attacks and Dark Web Scanning, with monthly uptime of 100% during the period of contract which shall be calculated on a quarterly basis.	Uptime of 100% is technically impossible, Request KaGB to reconsider an uptime of 98% calculated month.	Bidder to comply with RFP terms
44	19.3 Penalty for each Incident happened and not reported:	15	19.3 Penalty for each Incident happened and not reported: Entire section	Internet is huge and covering the internet both surface and dark web for incidents would be technically impossible. There will always be some miss. Hence, Request KaGB to remove this clause	Bidder to comply with RFP terms
45	19.4 Penalty for failure to resolve incidences (to be calculated on quarterly average basis)	16	19.4.1 Bidder should resolve the incidents as reported in Clause 19.3 within stipulated timelines. Failure to resolve incidents like phishing, pharming, malware, brand abuse, etc., the bidder shall be liable to pay penalty at the rates specified below: Resolution time Penalty amount Resolution time Penalty amount Within 240 minutes No penalty 241 to <300 minutes 1.00% (+ GST) of Total Quarterly Payment of In-scope services 301 to <360 minutes 2.00% (+ GST) of Total Quarterly Payment of In-scope services 361 to <420 minutes 3.00% (+ GST) of Total Quarterly Payment of In-scope services 421 to <480 minutes 4.00% (+ GST) of Total Quarterly Payment of In-scope services 481 to <540 minutes 5.00% (+ GST) of Total Quarterly Payment of In-scope services	The incident response would be in form of Takedowns of phishing sites, fake apps, brand incident. The Turn around time of takedowns are technically impossible and request KaGB to simplify the penalties. We advise of the below practical Turn Around Time (TAT), Hope this is acceptable with KaGB for takedowns: Trademark Takedown - Social Media within 48 -72 hours Copyright takedown - Social Media within 48 -72 hours Infringing website - Deactivation from non-compliant registrars or in regions with more complicated laws Fraudulent website (ISP level) within 2-7 weeks Fake or Infringing website deactivation within < 2 weeks Copyright takedown using DMCA within < 72 hours Host content Takedown within < 1 week Fake Mobile app takedown within < 1 week	Bidder to comply with RFP terms
46	19.4 Penalty for failure to resolve incidences (to be calculated on quarterly average basis)	16	19.4.2 If resolution time exceeds beyond 9 hours (540 minutes) from the date and time of identification, penalty equivalent to 10% plus GST of Quarterly Payment of in-scope services will be charged. In case an incident is not closed within a period of 7 days from the date and time of its identification then Bank will reserve the right to get such incident closed from other parties, expenses for which shall be recovered from the vendor.	The Turn around time of takedowns and penalties are technically impossible to comply, Request KaGB to simplify the penalties. Request below amendments: SLA Measurement & Failure Indicator: Takedown of Phishing sites %age of phishing sites taken down from the time of detection – Takedown within 48-72 hours or Update follow up status every 24 hours Penalty: Maximum 15 takedown violations are accepted in a quarter. For every single violation after that, penalty will be charged 10% of per takedown price, Penalty Payment up to maximum 10% of overall takedown price per quarter in form of service extension. The OEM would not bear any expenses, In case an incident is not closed within a period of 7 days. As takedowns are factor of many variables.	Bidder to comply with RFP terms
47	19.4 Penalty for failure to resolve incidences (to be calculated on quarterly average basis)	16	19.4.5.The maximum penalty levied under this clause shall not be more than 20% plus applicable taxes of the Total Quarterly Payment.	Request below amendments: Maximum 15 takedown violations are accepted in a quarter. For every single violation after that, penalty will be charged 5% of per takedown price, Penalty Payment up to maximum 5% of overall takedown price per quarter in form of service extension.	Bidder to comply with RFP terms

48	19.5 Penalty for failure to resolve Trojan Malware incidents (To be calculated on incident basis):	17	The bidder should resolve the Trojan Malware incidents within 24 hours of detection. Penalty at the rate of 10% of Quarterly Payment of Website scanning services will be charged if the delay in resolution of Trojan incidents is more than 24 hours but less than 48 hours. In case of resolution time is more than 48 hours, and less than a week, penalty at the rate of 20% (+ GST) of Quarterly Payment of Website scanning services will be charged. If the resolution time is more than One week, penalty at the rate of 100% of Quarterly Payment of Website scanning services will be charged.	Request Bank to remove this clause	Bidder to comply with RFP terms
49	19.6 Penalty on Deep Web/ Darknet services	17	19.6.1 The bidder needs to monitor for sensitive data on Dark/deep web and inform the bank immediately for sensitive data available in dark web. If selected bidder fails to detect and inform bank about any incident in Dark web/ Darknet prior to bank detecting/ any other party/ agency informing bank about any of the incidents in Darkweb/ Darknet then penalty will be as under: Incident based Penalty For each undetected incident 1.00 % (+ GST) of Total Quarterly Payment Maximum cap for penalty is 5% of the Total Quarterly Payment The bidder also needs to submit bi-weekly / weekly reports on the incidents of data compromise detected on Dark Web. If there are more than 5 such undetected incidents reported to the vendor, then bank reserves the right to review to continue with the services of the shortlisted vendor.	Deep and Dark web is huge and covering the entire Deep and Dark web for incidents would be technically impossible. There will always be some miss. Hence, Request KaGB to remove this clause	Bidder to comply with RFP terms
50	19.7 Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	17	Resolution time Penalty amount Within 4 hours No penalty More than 4 hours, but less than 8 hours 0.25% + GST of Total Quarterly Payment More than 8 hours, but less than 24 hours 0.50% + GST of Total Quarterly Payment More than 24 hours, but less than 48 hours 1.00% + GST of Total Quarterly Payment More than 48 hours, but less than 72 hours 2.00% + GST of Total Quarterly Payment More than 72 hours 10.00% + GST of Total Quarterly Payment	The incident response would be in form of Takedowns of phishing sites, fake apps, brand incident. The Turn around time of takedowns are technically impossible and request KaGB to simplify the penalties. We advise of the below practical Turn Around Time (TAT), Hope this is acceptable with KaGB for takedowns: Trademark Takedown - Social Media within 48 -72 hours Copyright takedown - Social Media within 48 -72 hours Infringing website - Deactivation from non-compliant registrars or in regions with more complicated laws Fraudulent website (ISP level) within 2-7 weeks Fake or Infringing website deactivation within < 2 weeks Copyright takedown using DMCA within < 72 hours Host content Takedown within < 1 week Fake Mobile app takedown within < 1 week	Bidder to comply with RFP terms
51	19.7 Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	18	The maximum penalty levied shall not be more than 10% plus applicable taxes of the Total Quarterly Payment.	Request below amendments: Maximum 15 takedown violations are accepted in a quarter. For every single violation after that, penalty will be charged 5% of per takedown price, Penalty Payment up to maximum 5% of overall takedown price per quarter in form of service extension.	Bidder to comply with RFP terms
52	19.7 Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	18	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.	Phishing site blocking and takedowns are different. CloudSEK offers takedowns for phishing sites which is a preferred by Major banks and BFSI clients. As per the penalty, below would be advised. Maximum 15 takedown violations are accepted in a quarter. For every single violation after that, penalty will be charged 5% of per takedown price, Penalty Payment up to maximum 5% of overall takedown price per quarter in form of service extension.	Bidder to comply with RFP terms
53	19.7 Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	18	The Phishing site, mobile app should not appear again within 12 months from the date of taking down. In case the Phishing site and/or mobile app reappear, then, the bidder must take down the same at no extra cost to the Bank.	This is not something in the control of the OEM, however, The OEM would ensure bringing down the reactivated phishing site/mobile app at earliest which was earlier detected as phishing site/fake mobile app. If the same site/app becomes active again within a period of 90 days of its taking down, it would not be treated as a new incident and would be taken down as part of original incident.	Bidder to comply with RFP terms
54	19.7 Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under	18	Phishing sites in web on all major browsers such as Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera, etc.	Phishing site blocking and takedowns are different. CloudSEK offers takedowns for phishing sites which is a preferred by Major banks and BFSI clients.	Bidder to comply with RFP terms

55	19.8 Penalty for failure to maintain response time for scanning of Banks website for defacement (to be calculated on incident basis)	18	19.8 Penalty for failure to maintain response time for scanning of Banks website for defacement (to be calculated on incident basis) A genuine act of defacement on Bank's websites should be detected within 30 minutes of the incident. Penalty at the rate of 2% of Total Quarterly payment will be charged for delay in detection of defacement for more than 30 minutes but less than 1 hour. In case of response time more than 1 hour the penalty at the rate of 5% of Total Quarterly payment will be charged. If the response time is more than 24 hours, penalty at the rate of 10% of Total Quarterly payment will be charged.	Request Bank to remove this clause	Bidder to comply with RFP terms
56	20.9.14 Right to alter the number of websites and apps:	21	The Bank reserves the right to alter the number of websites and apps specified in the tender in the event of changes in plans of the Bank. Any decision of the BANK in this regard shall be final, conclusive and binding on the bidder. The bank reserves the right to place order for these additional numbers of websites and apps at the agreed price during the contract period with the same terms and conditions.	Increase in scope would have an impact on the compute, delivery and hence an implication in the overall pricing and would be conveyed to KaGB and agreed by KaGB.	Bidder to comply with RFP terms
57	ANNEXURE 02 - A - General Features - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	2- 24*7*365 real time monitoring and support for all the services covered for:	Request below amendments: 24*7*365 near - real time monitoring and support for all the services covered for:	Bidder to comply with RFP terms
58	ANNEXURE 02 - A - General Features - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	6 - Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	Request Bank to remove this clause	Bidder to comply with RFP terms
59	ANNEXURE 02 - A - General Features - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	12 - Solution should provide for identification of fake recruitment schemes claiming affiliation with the bank.	This would be supported using fake domain, as fake domains are used to run fake recruitment schemes claiming affiliation with the bank.	Ok with Bank as long as the requirement is met
60	ANNEXURE 02 - A - General Features - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	16 -Vendor should assist the Bank in forensic investigation for inscope domains and mobileapps.Vendor should note that forensic analysis or investigation will not be entrusted on them , however the Vendor should provide support and details for assisting the Bank in analysis and investigation.	Once an incident is identified, CloudSEK XVigil's detailed incident screen list all the possible forensic information such as the IP addresses associated with the phishing domain, DNS records and WHOIS data of the domain. It will also have an option to download the incident report and an option to view the screenshots along with the timestamps of the screenshots. Any custom forensic request would be out of scope.	Bidder to comply with RFP terms
61	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	1 - The solution should support industry standard reporting including OWASP top 10 categorizing	Request below amendment: The solution should support industry standard reporting including some of the OWASP top 10 categorizing, CVSS etc.	Bidder to comply with RFP terms
62	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	2 - The solution should support Authenticated scanning with different authentication methods including Form, HTTP basic, NTLM and digest	Request Bank to remove this clause	Bidder to comply with RFP terms
63	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	3 - The solution should have Malware scanning feature	Request Bank to remove this clause	Bidder to comply with RFP terms
64	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	5 - Bidder must provide solution for 24X7 monitoring for Malicious Mobile Code (MMC) infection of the websites i.e. 24x7x365 monitoring / scanning of internet facing web applications of the Bank for real time detection of malware injection.	Request Bank to remove this clause	Bidder to comply with RFP terms
65	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	7 - The bidder has also to suggest suitable counter measures to safe guard against such threats (MMC) and advise /assist to eradicate it on utmost priority.	Request Bank to remove this clause	Bidder to comply with RFP terms
66	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	8-Monthly and other ad-hoc reports to be provided as per the requirement and format provided by the Bank.	All the reports are automated and can be scheduled in the platform either Daily/Weekly/Monthly. Hope this is fine with KaGB	Ok with Bank as long as the requirement is met
67	ANNEXURE 02 - B - Anti Malware and Anti Website Defacement - KaGB: Project Office:RFP:01/2021-22 dated 23.06.2021	NA	11- Blocking of the phishing sites in webbrowsers.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.	Request below amendments as naming providers very specifically would be challenging for compliance, as OEM/Services providers would have relationship with many service providers and but not limited to the mentioned: The blocking network from the service provider should include world's leading browser developers hosting providers/third party play stores/Social Media platforms, and others and should support multilingual analysis and operational capabilities.	Bidder to comply with RFP terms
68	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	3 Implementation of real time detection mechanisms and alerts.	Request below amendments: Implementation of real time detection mechanisms and alerts.	Not a Valid Query

69	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	4 Implementation of watermark and other means/techniques for each website.	Request below amendments for clarity in scope and further delivery: " For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers/ Signature Approach/ Logo Matching etc. without compromising the detection of phishing sites"	Bidder to comply with RFP terms
70	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	5 Performing the services for detecting anti - phishing mechanisms such as referrer logs, watermarks etc.	Request below amendments for clarity in scope and further delivery: " For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers/ Signature Approach/ Logo Matching etc. without compromising the detection of phishing sites"	Bidder to comply with RFP terms
71	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	6 Track hosting of phishing sites through implementation of watermark and other Means.	Request below amendments for clarity in scope and further delivery: " For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers/ Signature Approach/ Logo Matching etc. without compromising the detection of phishing sites"	Bidder to comply with RFP terms
72	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	8 Provide need based analysis on suspicious e-mail messages.	The solutions is an external threat monitoring platform. Does not monitor internal mailbox , hence this would be out of scope	Refer to Amendment 01
73	ANNEXURE 02 - C Early Phishing Detection: KaGB: Project Office:RFP:01/2020-21	NA	9 Monitoring spam traps to detect phishing mails	The solutions is an external threat monitoring platform. Does not monitor internal mailbox , hence this would be out of scope	Refer to Amendment 01
74	ANNEXURE 02 - G Brand Protection and Monitoring: KaGB: Project Office:RFP:01/2020-21	NA	1 24x7 anti-phishing , anti-Trojan , and anti-malwareservice to scan critical websites and Mobile Apps identified by Bank for the tenure of the Contract.	Request Bank to remove this clause	Bidder to comply with RFP terms
75	ANNEXURE 02 - G Brand Protection and Monitoring: KaGB: Project Office:RFP:01/2020-21	NA	2 Any newly launched websites and Mobile Application by the Bank in future to be scanned without any cost incurred to the Bank	Increase in scope would have an impact on the compute, delivery and hence an implication in the overall pricing and would be conveyed to KaGB and agreed by KaGB.	Refer to Amendment 01
76	ANNEXURE 02 - G Brand Protection and Monitoring: KaGB: Project Office:RFP:01/2020-21	NA	21 Ability to monitor all kind of incidents given below: 21.3 Trojan	Request Bank to remove this clause	Bidder to comply with RFP terms
77	ANNEXURE 02 - G Brand Protection and Monitoring: KaGB: Project Office:RFP:01/2020-21	NA	24 Legal support in the form of communication with CERTin / Cybercrime (with special permission from the Bank) . Technical support should be provided on a continuous basis	CloudSEK would be able to assist client for coordination with law enforcement agencies like CERT /Cyber Crime Cells on special requests only.	Ok with Bank as long as the requirement is met
78	General Query	NA	No. of concurrent user	Request Bank to clarify	Would be Provided to Successful Bidder if Required
79	General Query	NA	Current firewall (if Applicable)	Request Bank to clarify	Would be Provided to Successful Bidder if Required
80	General Query	NA	Any Web Security or Gateway Security deployed (if Applicable)	Request Bank to clarify	Would be Provided to Successful Bidder if Required
81	General Query	NA	No. of Application servers to be monitored.	Request Bank to clarify	Would be Provided to Successful Bidder if Required
82	General Query	NA	Antivirus deployed (if Applicable)	Request Bank to clarify:	Would be Provided to Successful Bidder if Required
83	General Query	NA	Any other network component they want to monitor.	Request Bank to clarify:	Would be Provided to Successful Bidder if Required
84	General Query	NA	Details of any current security measures (if Applicable).	Request Bank to clarify:	Would be Provided to Successful Bidder if Required
85	19.3.1		The bidder shall alert &– report to the Bank within 30 minutes of an attack/compromise.	The time of attack is often unknown. How do we define start of attack? When spam is sent? Phishing site hosted? Bank should revise to a quantity/rate of missed detection, rather than time to report, as T zero is unknown/undefined	Bidder to comply with RFP terms
86	19.3.2	15	If the bidder fails to report incident like Phishing, Pharming, Brand abuse, Trojan, Malware, Website defacement (To be calculated for each and every incident) that has occurred and not reported to the Bank, penalty would be as under	Placing a timed parameter into a missed detection SLA is problematic, please defined Time = Zero (Start), Request Bank to clarify: How do we calculate Time = Zero	Bidder to comply with RFP terms
87	19.5	17	Penalty for Delay in takedown of Phishing sites and fraudulent mobile apps specifically targeting Banks (Standalone attacks) shall be calculated on an incident basis as under		Not a Valid Query
88	Eligibility criteria; 10	55	The bidder must have minimum five (5) IT Security professionals, on payroll, having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B. Tech)/ Master's in computer application (MCA) along with certifications like CISA/ CISSP/ CISM/CEH/CCNP.	Request Bank to change it to : The bidder must have minimum **two (2) IT Security professionals**, on payroll, having degree equivalent to Bachelor of Engineering (B.E.)/Bachelor of Technology (B. Tech)/ Master's in computer application (MCA) along with certifications like CISA/ CISSP/ CISM/CEH/CCNP.	Bidder to comply with RFP terms
89	19.2 Penalty for delay in Implementation and Delivery of services	**15**	Penalties for delay in implementation and delivery of services as specified in clause 18 would be as under, subject to a cap of 5% plus GST on the Total Project Cost:	Request Bank to change it to :Penalties for delay in implementation and delivery of services as specified in clause 18 would be as under, subject to a cap of **2% plus GST** on the Total Project Cost:	Bidder to comply with RFP terms
90	19.3.3 Penalty for delay in Implementation and Delivery of services	**15**	The maximum penalty levied under this clause shall not be more than 5% plus applicable taxes of the Total Quarterly Payment.	Request Bank to change it to : The maximum penalty levied under this clause shall not be more than **2% plus** applicable taxes of the Total Quarterly Payment.	Bidder to comply with RFP terms

91	19.4.2	**16**	If resolution time exceeds beyond 9 hours (540 minutes) from the date and time of identification, penalty equivalent to 10% plus GST of Quarterly Payment of in-scope services will be charged.	Request Bank to change it to: If resolution time exceeds beyond 9 hours (540 minutes) from the date and time of identification, penalty equivalent to **5% plus GST of Quarterly Payment of in-scope services** will be charged.	Bidder to comply with RFP terms
92	19.4.5.	**16**	The maximum penalty levied under this clause shall not be more than 20% plus applicable taxes of the Quarterly Payment of in-scope services .	Request Bank to change it to: The maximum penalty levied under this clause shall not be more than **10% plus applicable taxes** of the Quarterly Payment of in-scope services .	Bidder to comply with RFP terms
93	19.5 Penalty for failure to resolve Trojan Malware incidents (To be calculated on incident basis):	**17**	The bidder should resolve the Trojan Malware incidents within 24 hours of detection. Penalty at the rate of 10% of Quarterly Payment of Website scanning services will be charged if the delay in resolution of Trojan incidents is more than 24 hours but less than 48 hours. In case of resolution time is more than 48 hours, and less than a week, penalty at the rate of 20% (+ GST) of Quarterly Payment of Website scanning services will be charged. If the resolution time is more than One week, penalty at the rate of 100% of Quarterly Payment of Website scanning services will be charged.	Request Bank to amend it as: The bidder should resolve the Trojan Malware incidents within 24 hours of detection. Penalty at the rate of **5% of Quarterly Payment of Website scanning services** will be charged if the delay in resolution of Trojan incidents is more than 24 hours but less than 48 hours. In case of resolution time is more than 48 hours, and less than a week, penalty at the rate of **10% (+ GST) of Quarterly Payment of Website scanning services** will be charged. If the resolution time is more than One week, penalty at the rate of 100% of Quarterly Payment of Website scanning services will be charged.	Bidder to comply with RFP terms
94	20.1 Payment Terms	**19**	Payment shall be released quarterly in arrears at actuals after completion of monitoring services and submission of deliverables (reports and recommendations) and acceptance of the same by the Bank officials for the respective area of service.	Request Bank to amend the payment terms as: **90% of the product cost** shall be released **after delivery of the product** and **10%** of the product cost shall be released **after implementation** of the product. **Service Payment** shall be released **quarterly in advance** at actuals after completion of monitoring services and submission of deliverables (reports and recommendations) and acceptance of the same by the Bank officials for the respective area of service.	Bidder to comply with RFP terms
95	20.8 Payment Terms	**19**	No payment shall be released for reopen incidents. (An incident shall be counted as reopen incident if it meets the following criteria: a. Incident with same IP address b. Incident with same Fully Qualified Domain Name (FQDN) c. A reopen incident within 180 days of the previous incident closure will not be treated as separate incident for purpose of calculation of number of incidents for payment.)	Request Bank to Remove this clause	Bidder to comply with RFP terms
96	18; Project Implementation Timeline	**14**	The monitoring services for Anti-Phishing, Anti-pharming, Anti-Malware, Rogue Attacks, Anti-Trojan and Anti Website defacement managed services should start within 7 days from the date of acceptance of the purchase order.	Request Bank to amend it as :The monitoring services for Anti-Phishing, Anti-pharming, Anti-Malware, Rogue Attacks, Anti-Trojan and Anti Website defacement managed services should start **within 21 days** from the date of acceptance of the purchase order.	Bidder to comply with RFP terms
97	1. Schedule of Activities, Events and Timeline	**5**	Application Fees (Non-Refundable) Rs. 10,000 + applicable GST	Request Bank to change it as: Application Fees (Non-Refundable) Rs. 2,000 + applicable GST	Bidder to comply with RFP terms
98	6.2	10	The selected bidder should respond immediately upon detection of any of the above attacks and should work to shut down/take-down the detected site, anywhere in the world also within the minimum possible time as specified in SLA on Real-Time Basis. For the purpose of detection bidder may use any technique or combination of techniques such as but not limited to scanning of web server logs and / or Digital watermarking/ or monitoring chat rooms used by hackers etc.	if the expectation is real-time, then the sizing will be of super criticality. We will rely heavily on the SIEM tool and it should have a underpinning performance for us to be able to respond/react immediately. What is the current performance of the SIEM/AV/Firewall/IDS/IPS tools?	Would be Provided to Successful Bidder if Required
99	6.3	10	The bidder should ensure bringing down the reactivated phishing site at earliest which was earlier detected as phishing site. If the same site becomes active again within a period of 180 days of its taking down, it should not be treated as a new incident and should be taken down as part of original incident.	Does the bank have underpinning contract with different ISPs/DNS registrar in India to accomplish the same. We would use the same to accomplish the task. However it should be noted that the SLA will have a dependency on the type of contract that Bank has	Bidder to comply with RFP terms
100	6.4	10	Continuous scanning of all the websites / mobile apps of the Bank to detect any type of blacklisted links, suspicious activities including SQL injection/ app reverse engineering etc. reporting to the Bank the exact nature and location of the infection for speedy removal of the infection / abnormality.	This kind of testing/monitoring requires that the application architecture be discussed with vendor. Also This is indicating that the vendor has to perform a DAST on the specified websites and provide results on continuous basis. It should be noted that any kind of vulnerability of penetration testing has to be validated before it can be remediated. The scans are usually done on pre-production to avoid any outages.	Bidder to comply with RFP terms
101	6.5	10	Proactive monitoring of Major Mobile App stores and blocking/shutting down of malicious App/Trojan used for Bank.	Needs further discussion. How any other applications can access the bank's infrastructure - what kind of device/user/customer authentication is provided? What if the customer does modification to the application code after all the installation is done?	Not a Valid Query
102	6.6	10	Gathering the Forensic information such as IP address, exact URL, source of attack, images, screen shots, email, account details, card details, compromised data etc. from the attacks and sharing the same with the Bank.	OK	Not a Valid Query
103	6.7	10	Pushing the bait details and counter measures (like login through many dummy users to identify the source and try to shutdown) in the fraudulent sites.	Need further discussion	Not a Valid Query
104	6.8	11	Reporting to Bank in line with regulatory requirements about all the attacks and providing detailed information through email, dashboard, SMS alerts, phone calls etc. Details of compromised accounts should be shared immediately with the Bank. Conference call facility with the vendor team should available to bank in case requirement arises.	OK - May need further investment	Not a Valid Query
105	6.9	11	Take up and coordinate the cases with CERTs and / or other legal agencies as per the format provided by the Bank.	Will need additional effort and we need to cost it per interaction so that we don't lose out on the effort.	Bidder to comply with RFP terms

106	6.10	11	Monthly and other ad-hoc reports to be provided as per the requirement and format provided by the Bank.	One monthly report and limited to 5 adhoc reports	Bidder to comply with RFP terms
107	6.11	11	Vendor will be required to submit monthly analysis and fraud intelligence reports (both high level/summarized and low level/detailed) to bank.	Should be included in 6.10 only	Bidder to comply with RFP terms
108	6.12	11	Providing bank with review and advisories for phishing, incidents and how to avoid such incidents in future.	Will be provided on a consulting basis. Please check language since the expectation seems to be to provide this as a apart of the contract itself	Bidder to comply with RFP terms
109	6.13	11	Vendor should provide Darknet services and monitor Darkweb for the information and documents related to Banks and share the data related to cards (Debit Cards, Credit Cards, Financial Information etc.) with the Bank on daily basis	it is possible that there will not be dialy exposure of bank cards in bulk. We should restrict it to the exposure happening due to a XFR from bank and not from other sources.	Bidder to comply with RFP terms
110	6.14	11	Service provider should also purchase 3-4 samples if desired by the Bank to ascertain the genuineness of the data without any additional cost to the bank.	Need clarity	Not a Valid Query
111	6.15	11	The vendor needs to perform Darkweb/ Darknet forum monitoring for bank registered brand. The vendor should monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels where cyber-criminals congregate to sell/ buy services and tools and exchange knowledge for banks brand.	Only registered brand? Need to discuss this. This might be worded like this but they may interpret it to mean everything related to bank.	Not a Valid Query
112	6.16	11	Bank can also increase or decrease the scope of services during the period of contract with a notice of 30 days.	Can we negotiate 30 Days + transiton period of 60 days?	Bidder to comply with RFP terms
113	6.17	11	The detailed list of Bank 's websites & mobile apps will be provided to successful bidder. However, this list is subject to change. Bidder will be required to monitor all the domains of the Bank including new domains Bank may acquire during the period of contract. Additional Websites or Mobile Applications to be included immediately for Monitoring and Managed Services on receipt of official communication from Bank. Bidder has to monitor the domains of the Amalgamated entity, if any, during the period of contract	OK	Not a Valid Query
114	6.18	11	Services should not impact the working of any of the bank's website. Any configuration done on the bank's infrastructure for the purpose of monitoring and prevention of malicious threats should not impact or degrade the performance of the websites	Current baselines to be understood and comitted post proposing the change in architecture.	Not a Valid Query
115	6.19	11	Service provider should comply with any time-to-time advisories/ changes from regulatory agencies. It should make any necessary changes in the services accordingly and provide updated services to the bank without any additional cost.	Need clarity	Not a Valid Query
116	6.20	11	The services or portal should provide a realtime view of all the components of Bank's digital threat protection. An all-encompassing dashboard illustrates threat data, including volume by source and category, and takedown status. Users can also set up email alerts, create online or printer reports, request takedowns.	Data on the dashboard should be retained only for 30 day window. It will be updated as and when there are changes in any of the parameters that are monitored.	Bidder to comply with RFP terms
117	6.21	12	Domain, Brand protection & Social Media Impersonation Monitoring: Analysis of social networks such as Facebook, twitter, LinkedIn etc. and domain registrations to find fake social profiles, malicious mentions and similar domains that impersonate our Bank and compromise customer information.	Facebook to compromise customer data?	Bidder to comply with RFP terms
118	6.22.1	12	Alert within 30 minutes of attack/compromise.	We can accomplish this provided the current monitoring infrastructure is able to detect the attacks. Additionally, we should establish the efficacy of the current situation that the bank has already not been compromised. We will need a continuos monitoring on the SIEM as well.	Bidder to comply with RFP terms
119	6.22.2	12	Initial response to the incident within 30 minutes with action plan on taking down and other alternative response mechanisms. Initial response includes formulating the initial respons plan and discussion with Bank stakeholders for future course of action.	POA - needs agreement from all the stakeholders of bank for us to meet the SLA.	Bidder to comply with RFP terms
120	6.22.3	12	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.	Need further discussiom. We will not have control over browsers at large.	Bidder to comply with RFP terms
121	6.22.4	12	The phishing site, mobile app should not appear again within 12 months of taking down. In case site or mobile app reappears, the same has to be taken down at no extra cost to the Bank.	Not acceptable since new variant may be released within no time	Bidder to comply with RFP terms
122	6.22.5	12	Resolution of Trojan incidents with in 24hrs of detection.	Resolution will be followed-up with resolver groups and they should respond within the SLA.	Bidder to comply with RFP terms
123	6.22.6	12	In case of defacement of Bank's websites and corresponding web pages, the bidder should alert Bank over call within 30 minutes.	monitoring the websites where the bank is hosting their web pages need to be treated as different scope provided they are hosted on different third party providers.	Bidder to comply with RFP terms
124	6.22.7	12	The bidder to provide the comprehensive SLA in their proposal.	We will provide all the SLA's mentioned in the contract as per agreement.	Not a Valid Query
125	6.22.8	12	The bidder needs to monitor for sensitive data on Dark/Deep web and inform the Bank immediately for sensitive data available in dark web. The bidder also needs to submit biweekly/weekly reports on the incidents of data compromise detected on Darkweb.	Reporting will be in line with section 6.10	Bidder to comply with RFP terms

126	15		We will provide based on agreed T&C.	Unless otherwise explicitly agreed in contract, we will not perform certification of the deliveries to any of the certification bodies.	Bidder to comply with RFP terms
127	19.1	16	Planned down time due to bank's requirement/direction should not be calculated.	NEEDS TO BE DISCUSSDED	Not a Valid Query
128	19.3	16	The bidder shall alert &– report to the Bank within 30 minutes of an attack/compromise		Not a Valid Query
129	No.4	56	Turnover of Rs. 5 (Five) Crores per annum from IT sales in each of the last three financial years,	NEED TO CHANGE TO 3-3.5 CRORES SINCE WE ARE MSME WITH NSIC AND WOMEN DIRECTOR	Bidder to comply with RFP terms
130	23.23.1	52	The Selected Bidder has to inform change in the management of the company, if any, to the Bank within 30 days from the date of such change during the period of contract.	ITS PRACTICALLY NOT POSSIBLE SINCE WE NEED TO HAVE BANKS INTERNAL NETWORK SCAN REPORT AND WE NEED TO RUN COMPLETE COMPROMISE ASSESSMENT FOR COMPLETE INTERNAL NETWORK BEFORE DEPLOYING OUR SOLUTIONS	Not a Valid Query
131	21.7.18	31	The Selected Bidder shall install and commission the equipment/services, in terms of this RFP, at locations designated by Bank or at such Centers as Bank may deem fit and the changes, if any, in the locations will be intimated to the Bidder	SINCE WE RUN ALL THE BOM AS MANAGED SERVICE FROM OUR DC	Bidder to comply with RFP terms