Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
1	Page No. 2	Bid Details in Brief	Last Date of Submission of Bids	Request for the extension till 22nd March 2022	Bidder to comply with RFP Terms.
2	Page No.13	5.8	CBS system integrator and consultant	Can we know thw CBS system integrators name also the consultant.	Details will be shared with the selected bidder.
3	Page No.20	9.1 Training	Location of the training must be in Bengaluru.	Please confirm whether the training facilities (location, sitting arrangement, desktops etc) will be provided by KGB or not?	It is the responsibility of the selected bidder.
4	Page No. 27	15.1	15.1 This document can be downloaded from Bank's website https://karnatakagraminbank.com/, https://keralagbank.com/, https://canarabank.com/ . In that event, the bidders should pay the Application Fee of Rs. 59,000/- inclusive of GST at 18% (non-refundable) for tender document by means of DD drawn on any scheduled Commercial Bank in favor of Karnataka Gramin Bank, payable at Bengaluru, Karnataka and submit the same along with Part A-Conformity to Eligibility Criteria	It is a request that the bidders should pay the Application Fee of Rs. 59,000/- inclusive of GST at 18% (non-refundable) for tender document by means of DD **or NEFT**	Bidder to arrange only Demand Draft.
5	Page No. 29	23		Considering longer timelines in hardware delivery, kindly revise the timelines as below: 1. SIEM - T + 34 2. PIM - T + 28 3. Anti-APT - T + 22 4. VM - T + 18	Bidder to comply with RFP Terms.
6	Page No. 29	23.3 Project Timelines Table 5:	All the in-scope solutions should be implemented parallelly. PIM - T+20 Weeks Anti-APT - T+14 Weeks VM - T+10 Weeks	In current situation hardware delivery is taking 12 weeks. Hence, deploying solution within 12 weeks from acceptance of PO will be unrealistic. Requesting to please change the timeline of mentioned solutions.	Bidder to comply with RFP Terms.
7	Page No.30	24.Project Team Structure	All team resources during the implementation should be on the payroll of the SI or OEM / OSD.	Bidder request to relax the implementation team to partner outsource payroll as you know there are lot of challenges to get the in-house skill, knowledgeable, experience resources on each & every OEM technology.	Bidder to comply with RFP Terms.
8	Page No.31	25	Service Level Agreements	Requesting the Bank to modify the penalty cap from 10% to 5%	Bidder to comply with RFP Terms.
9	Page No.31	25	Service Level Agreements Penalties	Maximum penalty capping during AMC period will be same as during warranty period ? (During warranty period maximum penalty is capped up to 5% of total order value)	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
10	Page No.31	25	b) Non-compliance of the Supply/ delivery clause 45.2 (a) will result in the Bank imposing penalty of 0.50% on delay in delivery per week or part thereof, on the total cost of the each in-scope solution (As per Table 1: of Annexure-5 Commercial Bill of Material). c) Non-compliance to the implementation clause 45.2 (b) will result in the Bank imposing penalty of 0.50% on delay in implementation per week or part thereof, on the total implementation charges of each in-scope solution. (As per Table 2: of Annexure-5 Commercial Bill of Material).	As a SI, we are always trying to match bank's SLAs. However, in case there are any SLA breaches, we request bank to revise existing penalty clauses as below: b) Non-compliance of the Supply/ delivery clause 45.2 (a) will result in the Bank imposing penalty of **0.10%** on delay in delivery per week or part thereof, on the total cost of the each in-scope solution (As per Table 1: of Annexure-5 Commercial Bill of Material). c) Non-compliance to the implementation clause 45.2 (b) will result in the Bank imposing penalty of **0.10%** on delay in implementation per week or part thereof, on the total implementation charges of each in-scope solution. (As per Table 2: of Annexure-5 Commercial Bill of Material). d) Penalty would be levied for delivery, installation, and implementation delays for each solution and shall be a maximum of **5%** of the total cost and Implementation Charges of each in-scope solution (As per Table 1: & Table 2: of Annexure-5 Commercial Bill of Material) from the selected bidder.	Bidder to comply with RFP Terms.
11	Page No.31	25.1 Penalties / Liquidated damages for delay in Delivery and Installation of Hardware/Software would be as under	Penalty would be levied for delivery, installation, and implementation delays for each solution and shall be a maximum of 10% of the total cost and Implementation Charges of each in-scope solution	Bidder requests that maximum LD capping for delay in delivery, installation, and implementation should be 5% of the total cost and Implementation Charges of each in-scope solution	Bidder to comply with RFP Terms.
12	Page No.32	25.1.d	d) Penalty would be levied for delivery, installation, and implementation delays for each solution and shall be a maximum of 10% of the total cost and Implementation Charges of each in-scope solution (As per Table 1: & Table 2: of Annexure-5 Commercial Bill of Material) from the selected bidder.	d) Penalty would be levied for delivery, installation, and implementation delays ~~for each solution~~ and shall be a maximum of **5%** of the total cost and Implementation Charges for complete RFP scope ~~of each in-scope solution~~ (As per Table 1: & Table 2: of Annexure-5 Commercial Bill of Material) from the selected bidder.	Bidder to comply with RFP Terms.
13	Page No.32	25.2 Penalties/Liquidated damages for not maintaining uptime during operational phase would be as under:	Table – 6: SLAs for Solution Uptime	Bidder request to add the clause that "Standalone Deployments will not be part of Solution uptime penalties."	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
14	Page No.32	25.2 e	e) The percentage uptime is calculated on monthly basis as follows: (Total contracted hours in a month – Downtime hours within contracted hours) * 100 Total contracted hours in a month	Request to exclude planned downtimes as well from calculations	Please refer clause 25.2 (e) -Note for clarification.
15	Page No.33	1	Table – 6: SLAs for Solution Uptime Solution Uptime 99.9% and above NA 98% to 99.89% 5% 95% to 97.99% 8% Below 95% 15%	The requested uptime is very stringent. Please relax this as below: Solution Uptime 99.5% and above NA 98% to 99.49% 1% 95% to 97.99% 3% Below 95% 5%	Bidder to comply with RFP Terms.
16	Page No.51	45. Delivery, Installation, Integration and Commissioning	a) Supply of Hardware and Software items: Within 8 weeks from the date of acceptance of Purchase Order	Requesting you to modify the clauses as "a) Supply of Hardware and Software items: Within 12 weeks from the date of acceptance of Purchase Order"	Bidder to comply with RFP Terms.
17	Page No.51	45. Delivery, Installation, Integration and Commissioning	Supply of Hardware and Software items: Within 8 weeks from the date of acceptance of Purchase Order	Owing to uncertainty owing to covid situation, OEMs are unable to commit to delivery timelines. Bidder requests to amend the clause as - Supply of Hardware and Software items: Within 14-16 weeks from the date of acceptance of Purchase Order	Bidder to comply with RFP Terms.
18	Page No.51	Point No. 45.2 a	Supply of Hardware and Software items: Within 8 weeks from the date of acceptance of Purchase Order	Request Bank to Increase delivery time lines to 16 Weeks	Bidder to comply with RFP Terms.
19	Page No.51	45. Delivery, Installation, Integration and Commissioning	Installation, Configuration, and Implementation: as per Timelines defined in the Clause no. 23.	Bidder requests that the installation, configuration and implementation timelines be considered as per clause no. 23 post supply and delivery of in scope hardware and software items.	Bidder to comply with RFP Terms.
20	Page No.51	Point No. 45.2 b	Installation, Configuration, and Implementation: as per Timelines defined in the Clause no. 23.	Request Bank to Consider the installation Configuration and Implementation from the date of felivery of the hardware and software.	Bidder to comply with RFP Terms.
21	Page No.53	50	Payment Terms - SIEM	Requesting Bank to Modify Payment terms for SIEM from 30%, 60% and 10% to 75%, 15% and 10% for Delivery, Implementation and Warranty.	Bidder to comply with RFP Terms.
22	Page No.53	Payment Terms, Table 12 , a, delivery	Percentage of Payment As per Table 1.1 of Annexure-5 Commercial BoM * Delivery 60%	We request Amendment as follows Upon delivery :80%	Bidder to comply with RFP Terms.
23	Page No. 53	50	Payment Terms - On Delivery - 60 % of payment	Please revise the payment terms to 90% payment on delivery of hardware for both SIEM and PIM.	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
24	Page No.53	50. Payment Terms	Payment Terms for SIEM:	We request bank to amend the clause as under : **Delivery** - 70% - After complete delivery of all hardware and software and Licenses. **Integration and Implementation**: 20% - After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work. **Sign off:** 10% - After completion of user acceptance and final sign off. Since bidder is already submitting a PBG for the total contract, any additional PBG requirement for release of payment should be removed.	Bidder to comply with RFP Terms.
25	Page No.54	Payment Terms, Table 12 b)Integration and Implementation	Percentage of Payment As per Table 1.1 of Annexure-5 Commercial BoM * 30%	We request Amendment as follows Integration and Implementation : 10%	Bidder to comply with RFP Terms.
26	Page No.54	50. Payment Terms	Table 13: Payment Terms for PIM, Anti-APT & VM:	We request bank to amend the clause as under : **Delivery** - 70% - After complete delivery of all hardware and software and Licenses. **Integration and Implementation**: 20% - After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work. **Sign off:** 10% - After completion of user acceptance and final sign off. Since bidder is already submitting a PBG for the total contract, any additional PBG requirement for release of payment should be removed.	Bidder to comply with RFP Terms.
27	Page No.55	Payment Terms, Table 12	AMC/ATS Charges (if contracted) will be released quarterly in arrears after completion of warranty period of Three Years.	We request amendment as below AMC/ATS Charges (if contracted) will be released on yearly advance basis for the all the software and hardware components. For Manpower , payment will ion quarterly in advance	Bidder to comply with RFP Terms.
28	Page No.65	76. Force Majeure	For the purpose of this clause, "Force Majeure" shall mean an event beyond the control of the selected bidder, due to or as a result of or caused by acts of God, wars, insurrections, riots, earthquake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the selected bidder, resulting in such a situation	In view of ongoing Covid-19 situation, bidder requests to include epidemic / pandemic situation in Force Majeure clause	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
29	Page No.69	Annexure 1, Table-14, Sr No.2	The Bidder/Bidder's Parent organization should have a minimum turnover of INR Twenty Five (25) Crores per annum from information security related services and products in any three out of last Five (5) financial years (2016-17, 2017-18, 2018-2019, 2019-20 and 2020- 21).	We request amendment to this clause as follows The Bidder/Bidder's Parent organization should have a minimum turnover of INR TEN (10) Crores per annum from information security related services and products, Managed IT Services contracts in any three out of last Five (5) financial years (2016-17, 2017-18, 2018-2019, 2019-20 and 2020- 21).	Bidder to comply with RFP Terms.
30	Page No.69	Annexure 1, Table-14, Sr No.2	The Bidder/Bidder's Parent organization should have a minimum turnover of INR Twenty Five (25) Crores per annum from information security related services and products in any three out of last Five (5) financial years (2016-17, 2017-18, 20182019, 2019-20 and 2020- 21).	Kindly amend the clause as : The Bidder/Bidder's Parent organization should have a minimum turnover of INR Eight (8) Crores per annum from information security related services and products in any three out of last Five (5) financial years (2016-17, 2017-18, 20182019, 2019-20 and 2020- 21).	Bidder to comply with RFP Terms.
31	Page No.69	Annexure 1, Table-14, Sr No.3	The Bidder/Bidder"s Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	**Please change as below** The Bidder/Bidder"s Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI/**Goverenment** sector in India.	Bidder to comply with RFP Terms.
32	Page No.69	Annexure 1, Table-14, Sr No.3	The Bidder/Bidder"s Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	Please Allow Consortium credential to fulfil these criteria.	Bidder to comply with RFP Terms.
33	Page No.69	Annexure 1, Table-14, Sr No.3	The Bidder/Bidder"s Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB /BFSI sector in India.	Kindly amend the clause as : The Bidder/Bidder"s Parent Company should have executed SOC as a service project during the period from 01.04.2016 to till date of RFP in any PSU/PSB /BFSI/ Govt sector in India.	Bidder to comply with RFP Terms.
34	Page No.69	Annexure 1, Table-14, Sr No.3	The Bidder/Bidder's Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	We request Amendment for this clause as below The Bidder/Bidder's Parent Company should have executed the SOC project which includes implementation of SIEM solution, during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI/Private and Corporate sector in India.	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
35	Page No.71	Annexure 1, Table-15, Sr No.1	a.) The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India. b.) The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India. Note: ¤ The bidder/bidder"s parent company should satisfy the eligibility criteria for both a) & b). ¤ The Bank will enter into contract with only the bidder and the responsibility of delivering the project as per SLAs defined in the RFP rests with the bidder. In case the bidder showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder only.	**Please change as below** a.) The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI/**Government** sector in India. b.) The bidder/bidder"s parent company should have implemented On-Premise SEIM and PIM/ **DLP/DDOS/Firewall/NAC/WAF** solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI /**Government** sector in India. Note: ¤ The bidder/bidder"s parent company should satisfy the eligibility criteria for both a) & b). ¤ The Bank will enter into contract with only the bidder and the responsibility of delivering the project as per SLAs defined in the RFP rests with the bidder. In case the bidder showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder only.	Bidder to comply with RFP Terms.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
36	Page No.71	Annexure 1, Table-15, Sr No.1	a.) The bidder/bidder‟s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India. b.) The bidder/bidder‟s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India. Note: ▫ The bidder/bidder‟s parent company should satisfy the eligibility criteria for both a) & b). ▫ The Bank will enter into contract with only the bidder and the responsibility of delivering the project as per SLAs defined in the RFP rests with the bidder. In case the bidder showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder only.	Please Allow Consortium credential to fulfil these criteria.	Bidder to comply with RFP Terms.
37	Page No.71	Annexure 1, Table-15, Sr No.1	a.) The bidder/bidder's parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India.	We request Amendment for this clause as below a.) The bidder/bidder's parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) / facility management service for Security solutions/ Managed IT Services in any PSU/PSB/BFSI /Private and Corporates in India.	Bidder to comply with RFP Terms.
38	Page No.71	Annexure 1, Table-15, Sr No.1	b.) The bidder/bidder's parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	We request Amendment for this clause as below The bidder/bidder's parent company should have implemented On-Premise SIEM / PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI/Private and Corporates sector in India.	Bidder to comply with RFP Terms.
39	Page No.71	Annexure 1, Table-15, Sr No.1	▫ The Bank will enter into contract with only the bidder and the responsibility of delivering the project as per SLAs defined in the RFP rests with the bidder. In case the bidder showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder only.	Need clarity on the term bidders parent company . Is bank referring to OEM of the SIEM solution as parent company and hence following condition are applicable **"In case the bidder showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder only.**" Kindly clarify on this clause	Bidder to comply with RFP Terms.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
40	Page No.71	Annexure 1, Table-15, Sr No.1	a.) The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India.	Kindly amend the clause as : The bidder/bidder"s parent company should be currently in the service of providing bidder's premise SOC as a service and facility management service for Security solutions in any PSU/PSB/BFSI/ Govt sector in India.	Bidder to comply with RFP Terms.
41	Page No.71	Annexure 1, Table-15, Sr No.1	a.) The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India.	Kindly amend the clause as : The bidder/bidder"s parent company should have SOC as a service solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI/ Govt sector in India.	Bidder to comply with RFP Terms.
42	Page No.71	Annexure 1, Table-15, Sr No.1	The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	Since SIEM and PIM solution may not have been supplied to same customer in the same RFP, we request bank to consider separate references for both. On those lines, kindly rephrase the criteria as below: The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of **RFPs** in any PSU/PSB/BFSI sector in India. **Both modules need not be part of single PO / Tender.**	**On premise SIEM & PIM Implementation experience in same/different organizations during the specifed period shall be considered.**
43	Page No.71	Annexure 1, Table-15, Sr No.1	Point 1, a & b clause - in any PSU/PSB/BFSI sector in India.	Bidder request to amend the clause as- PSU/PSB/BFSI/ Govt. sector in India.	Bidder to comply with RFP Terms.
44	Page No.71	Annexure 1, Table-15, Sr No.1	Point 1, a & b clause - in any PSU/PSB/BFSI sector in India.	Bidder understands that SIEM and PIM experience can be shwon in separate purchase orders. Pl confirm.	**On premise SIEM & PIM Implementation experience in same/different organizations during the specifed period shall be considered.**
45	Page No.72	Annexure 1, Table-15, Sr No.4	4.The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase	We would request bank to accept declaration from bidder to assign certified resources as per RFP requirement. However, since employees keep changing organizations, we may not be able to commit correct assignment of resources at current stage of tender. We can share CVs with bank once the PO is received before assigning to the project. Kindly consider our request.	**During implementation stage Certified resources should be made available. However, the certified resources mentioned in the self declarion submitted along with the bid need not be the same.**

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
46	Page No.72	Annexure 1, Table-15, Sr No.4	The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase	Please change as below The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution **at the time of implementation phase.** The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase	**During implementation stage Certified resources should be made available. However, the certified resources mentioned in the self declarion submitted along with the bid need not be the same.**
47	Page No.72	Annexure 1, Table-15, Sr No.4	The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase	Please Allow Consortium credential to fulfil these criteria.	Bidder to comply with RFP Terms.
48	Page No.72	Annexure 1, Table-15, Sr No.4	The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase.	Kindly amend the clause as : The bidder should have a minimum of 3 individuals with prior experience in implementation of SOC as a service. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase.	**During implementation stage Certified resources should be made available. However, the certified resources mentioned in the self declarion submitted along with the bid need not be the same.**
49	Page No.72	Annexure 1, Table-15, Sr No.4	The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution out of which a minimum of 2 individuals should be certified in the proposed solution. The bidders should deploy the certified and experienced resources during implementation at the Bank during the implementation phase.	Bidder should be given the choice to choose OEMs best suited for Banks environment, which is also cost effective and proven solution. Bidder requests that the clause be amended as The bidder should have a minimum of 3 individuals with prior experience in implementation of SIEM solution.	Bidder to comply with RFP Terms.
50	Page No.72	Annexure 1, Table-16, Sr No.1	Each of the proposed solution should have been implemented in a minimum of two PSU/PSB?BFSI Sector in India of which one should be scheduled Bank.	Please Allow Consortium credential to fulfil these criteria.	Bidder to comply with RFP Terms.
51	Page No.72	Annexure 1, Table-16, Sr No.1	Each of the proposed solutions should have been implemented in a minimum of Two PSU/PSB/BFSI sector in India of which One should be a scheduled bank.	Looking forward for the Startup Exemption only on this clause not on any of the technical capabilities.	Bidder to comply with RFP Terms.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
52	Page No.81	Annexure 6, Table-22, Sr No.A	Level 1 Resource - 24 * 7 * 365 monitoring from Banks C-SOC - Minimum 2 no. of seats each in shifts from 6 AM to 2 PM, 2 PM to 10 PM and 10 PM to 6 AM	For 24x 7 service window , you will require additional 3 resource apart from the dedicated 2 resource for each shift . Kindly include additional 3 resources as mandatory minimum resource count. This 3 resource will be for weekly off and leave management	Bidder to comply with RFP Terms.
53	Page No.85	Annexure 8, Table-28, Sr No.2	Bidders Past Experience - Minimum percentage for Technical Qualification is 60%	Even though bidder gets qualified its challenging to clear the Technical qualification as bidder should have minimum 3 PO and Signoff of each solution to achieve minimum 60% to get qualified. which will disqualify most of the bidders. Request Bank to remove the minimum percentage for Technical qualification from Bidder's past experience.	Bidder to comply with RFP Terms.
54	Page No.86	Annexure 8, Table-31	The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI sector in India	Bidder requests to amend the clause as - The bidder/bidder"s parent company should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any PSU/PSB/BFSI / Govt. sector in India	Bidder to comply with RFP Terms.
55	Page No.86	Annexure 8, Table-31	b.) The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	Bidder requests to amend the clause as - The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI / Govt.sector in India.	Bidder to comply with RFP Terms.
56	Page No.86	Annexure 8, Table-31	b.) The bidder/bidder"s parent company should have implemented On-Premise SIEM and PIM solution during the period from 01.04.2016 to till date of RFP in any PSU/PSB/BFSI sector in India.	Bidder understand that experience required for SIEM and PIM can be shown through separate purchase orders. Pl confirm.	**On premise SIEM & PIM Implementation experience in same/different organizations during the specifed period shall be considered.**
57	Additional clause		Site readiness	Bidder request for addition of a clause on site readiness Incase the site is not ready for implementation or delay from bank's side post 30 days from supply and delivery of in scope hardware and software items, bank will release the payment due against supply and delivery.	Bidder to comply with RFP Terms.
58	Page No.14	8.5	General Scope of Work for Each Solution In case of software-based solution, the bidder needs to propose the minimum level of hardware as below	Please confirm whether all the components of SIEM need to install on dedicated hardware or the solution can be virtualized?	It is up to the bidder to provide the best optimal solution to the Bank in order to meet the stated RFP requirements.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
59	Page No.14	8.5	General Scope of Work for Each Solution In case of software-based solution, the bidder needs to propose the minimum level of hardware as below	Please remove minimum hardware requirements for SIEM and other servers since these may vary from solution to solution. Bidder / OEM can provide undertaking for hardware sufficiency for required performance levels. Justification We Believe that every OEM has their own way of sizing the hardware because of differnece in architecture. The standardization of underlying hardware will have very different specifications with multiple support and sustenance	This is only minimum requirement that has been mentioned in RFP. It is up to the bidders to design their solution fulfilling the RFP requirements.
60	Page No.14	8.5.1	a) Minimum of 16 cores (Intel Xeon E5 based chip) and 32 GB of RAM and should be expandable to minimum 32 cores and 128 GB of RAM. Further, the bidder should ensure that minimum V4 / DDR4 are provided. b) All servers should at a minimum have 600 GB redundant SSD	The latest processors are with Icelake series. Please include the Icalake processor series in the minimum recommended specification details.	This is only minimum requirement that has been mentioned in RFP. It is up to the bidders to design their solution fulfilling the RFP requirements.
61	Page No.14	8.5.2	a) Intel Xeon quad core processor 2.4 GHz with 16 GB Ram (Rack mountable). b) All servers should at a minimum have 600 GB redundant SSD	The latest processors are with Icelake series. Please include the Icalake processor series in the minimum recommended specification details.	This is only minimum requirement that has been mentioned in RFP. It is up to the bidders to design their solution fulfilling the RFP requirements.
62	Page No.16	8.6.3 C-SOC Monitoring	Security Information & Event Management (SIEM) - C- SOC Monitoring	Please confirm whether the LED screens will be provided by bank or not? If bidder has to factor then please share the total count of LED screens that are required and the specifications of the same.	LED screens will be provided by the Bank.
63	Page No.16	8.6.3 C-SOC Monitoring	Security Information & Event Management (SIEM) - C- SOC Monitoring	Please confirm whether the Desktops will be provided by bank or not? If bidder has to factor then please share the total count of Desktops that are required and the specifications of the same	Desktops will be provided by the Bank.
64	Page No.16	8.6.4 Integration	Integration	What is the incident management and ticketing tool available with the bank?	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total SIEM solution.
65	Page No.16	8.6.5 Replication	Security Information & Event Management (SIEM) - Replication	What is the existing replication tool available with bank? please confirm whether bidder can utilize the existing tool for this RFP scope or not?	Bidder is expected to provide replication tool along with the SIEM solution.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
66	Page No.16	8.6.5 Replication	Security Information & Event Management (SIEM) - Replication	Replication: The logs collected by the SIEM log collector should be replicated across primary Data Canter, Disaster Recovery only." Request you to consider replication of logs for 3 months of logs on- box only. Rest of the logs can be collected on the single location where the logs are archived and offline storage is available. This is suggested for data management in a proper manner.	It is requested that the bidder should come with implementation strategies in accordance with the RFP requirements.
67	Page No.16	8.6.5 Replication	The logs collected by the SIEM log collector should be replicated across primary Data Center, and Disaster Recovery Centre	Is online replication is the requirement here? Please clarify.	Yes. Replication of logs should be on-premise.
68	Page No.16	8.6.5 Replication	Storage Replication - The bidder should ensure that there should be no data loss across DC and DRC. The logs should be in sync across DC and DRC.	DC & DRC are not at Metro Distance - Only Asynchronous Replication is possible between the storages.	Asynchronus replication should happen between DC & DRC without any data loss.
69	Page No.16	8.6.6 Storage	Storage	Storage:Will the Backup solution be provided by the bank for backing the logs ? Can the SI use the existing backup solution for taking backups ? If any additional device license is required, then SI can procure the same. Request the bank to share the backup solution being used by the bank so that SI can cnsider costs accordingly	Bank's existing backup solution is VEEAM.
70	Page No.16	8.6.6 Storage	The logs should be stored in tamper proof mechanism for online and archival storage. The archival storage should have "Write Once Read Many (WORM)", Encryption (or) Hashing, Index and Search, Retention and Disposal Functionality-Compression.	Archival storage - Deduplication as data reduction feature to achieve better space savings as compared to Compression. Kindly include the same in the RFP.	Bidder to comply with RFP Terms.
71	Page No.16	8.6.6 Storage	Tier-II Archival (5 Years), SAN Based with deduplication / compression capability (SATA / SAS / SSD) 7200 (or the latest version available) RAID5	Contradictory statement between Table-1 and Table 2 under 8.6.6 --- In Table 1, the specification mentioned as Tier-II Archival (5 Years), SAN Based with deduplication / compression capability (SATA / SAS / SSD). However in Table 2, the archival storage connectivity protocols is mentioned as CIFS, NFS & HTTP. The pprotocol specified for Archival storage is conflicting as SAN is a Block Storage. Archival Storage leverages Erasure Coding and not traditional RAID architecture. Kindly specify whether the bank is looking for NAS or SAN devices for the Storage.	Bank is looking for SAN devices for storage and refer Amendment No.1.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
72	Page No.16	8.6.6 Storage	Archival storage Connectivity Protocols to be supported: CIFS, NFS & HTTP.	Contradictory statement between Table-1 and Table 2 under 8.6.6 --- In Table 1, the specification mentioned as Tier-II Archival (5 Years), SAN Based with deduplication / compression capability (SATA / SAS / SSD). However in Table 2, the archival storage connectivity protocols is mentioned as CIFS, NFS & HTTP. The pprotocol specified for Archival storage is conflicting as SAN is a Block Storage. Archival Storage leverages Erasure Coding and not traditional RAID architecture. Kindly specify whether the bank is looking for NAS or SAN devices for the Storage.	Please refer Amendment No.1.
73	Page No.17	8.6.7 Packet Capture	Security Information & Event Management (SIEM) - Packet Capture	For Packet Capture please share the sizing of the packet capture solution: 1. What is the internet bandwidth? 2. What is the traffic throughput? 3. Amount and size of the packets so that Storage requirement can be sized based on 15 days raw packets and 30 days meta-data retention requirement.	1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps. 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
74	Page No.17	8.6.7 Packet Capture	Packet Catpure	For sizging the packet capture, please rpbvide the below details. 1. What is the LAN bandwidth (1 Gig / 10 Gig) of DC and DR? 2. What is the channel (Copper / Fibre) at DC and DR? 3. What is the percentage of utilization of Network at DC and DR? 4. How many zones to to be packet captured in the DC and DR? 5. What is the throughput of those zones under scope? 6. What is Bank's Internet Throughput?	1. LAN bandwidth : 1 Gig & 10Gig. 2. Channel : DC & DR : Copper and Fibre. Item no 3,4,5 will be provided to the selected bidder. 6. Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
75	Page No.17	8.6.7 Packet Capture	Clarification	For siziing the packet capture, please provide the below details. 1. What is the LAN bandwidth (1 Gig / 10 Gig) of DC and DR? 2. What is the channel (Copper / Fibre) at DC and DR? 3. What is the percentage of utilization (or in Mbps / Gbps) of Network at DC and DR to be captured? This is required for PCAP appliance sizing. Please provide the details or Can we assume 500 Mbps of traffic to be captured? 4. How many zones to be packet captured in the DC and DR? 5. What is the throughput of those zones under scope?	1. LAN bandwidth : 1 Gig & 10Gig. 2. Channel : DC & DR : Copper and Fibre. 3. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% Item no 4,5 will be provided to the selected bidder.
76	Page No.17	8.6.7 Packet Capture	Packet Capture	Please confirm the number of location is one(i.e. DC)	PCAP solutions to be placed both at Bank's DC and DR location.
77	Page No.17	8.6.7 Packet Capture	Packet Capture	Does the solution require in standalone mode?	Refer Annexure -4 . PCAP solution with HA in DC and Standalone in DR.
78	Page No.17	8.6.7 Packet Capture	Packet Capture	Do you require DC only setup? Or DR is required	Refer Annexure -4 . PCAP solution with HA in DC and Standalone in DR.
79	Page No.17	8.6.7 Packet Capture	Suggested Addition	The solution should have a feature rich Deep Packet Inspection Engine capable of dynamically detecting, decoding and, classifying over 4,500 protocols / applications. It will also help minimize application blind-spots.	Bidder to comply with RFP Terms.
80	Page No.17	8.6.7 Packet Capture	Suggested Addition	The solution must support port-agnostic protocol detection. The solution should be capable of detecting protocols and applications despite them using non-standard TCP/UDP ports.	Bidder to comply with RFP Terms.
81	Page No.17	8.6.7 Packet Capture	Suggested Addition	The solution should be capable of analysing recent traffic against a predefined rule base.	Bidder to comply with RFP Terms.
82	Page No.17	8.6.7 Packet Capture Clause a) & b)	a) The Solution must be capable of full packet capture and securely store these packets for a minimum of 30 days. b) Raw packets are to be stored for a period of 15 days and meta-data to be stored for a period of 30 days.	Request Bank to clarify on the packet capture retention, 15 days or 30days as these two specs are conflicting and modify the specs accordingly.	Please refer Amendment No.1.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
83	Page No.18	8.6.7 Packet Capture Clause c)	The solution should not have any restriction on the maximum packet size that can be captured.	Please highlight the total Throughput to be monitored (SPAN/Mirror):	1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps. 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
84	Page No.18	8.6.8 d)	The proposed solution should be able to integrate all the security devices/solutions being proposed as a part of the current RFP/existing and future security devices and solutions identified by the bank.	Does the Incident Management tool need to integrate with the different event / via API or can we assume that all event / alarm generation systems will send email notifications for any event / alarm which will be received by the Incident Management tool & converted to a ticket ?	The proposed solution should be able to flag an event and an automated notification to be sent to the respective team via email notification.
85	Page No.18	8.6.8 d)	The proposed solution should be able to integrate all the security devices/solutions being proposed as a part of the current RFP/existing and future security devices and solutions identified by the bank.	It is assumed that the incident ticket Priority / Severity will be entered manually by the SOC engineer once the incident is generated from any event / alarm received from the SOC systems. Hope this understanding is correct ?	The proposed SOC solution should be able to prioritize the events logged such has high, medium, and low. For further details please refer to the RFP requirements.
86	Page No.18	8.6.8 f)	The solution should be able to send the incident report in various forms like e- mail, SMS etc.	Reports will be sent via email but via SMS Incident Management tool will only send incident updates. Is our understanding correct for this point ?	Refer clause 8.6.8 (f).
87	Page No.18	8.6.8 Incident Management tool	Security Information & Event Management (SIEM) - Incident Management tool	Incident Management Tool asked as a part of SIEM, can bidder use an integrated tool with SIEM or bidder will propose it as a separate ITMS tool - Kindly Clarify ?	The bidder should consider it as part of the overall proposed SIEM solution.
88	Page No.18	8.6.8 Incident Management tool	Clarification	1. kindly confirm how many total number of agents / technicians are needed for the Incident Management tool 2. Is there any redundancy requirement for Incident Management tool (High Availability / DC-DR replication etc.) 3.kindly confirm if deployment needs to be done onsite or remote ?	1. The Bidder can consider the additional resources if required. Please refer to section 24.3 (b) and Annexure-6 for more details. 2. Redundancy is required for incident management tool. 3. Deployment needs to be done onsite.
89	Page No.18	8.6.8 Incident Management tool	Clarification	Kindly confirm if training need to consider for Incident Management and SSL decryption Tool	As part of overall SIEM solution Bank require training pertaining to those tools as well.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
90	Page No.18	8.6General Scope of Work for each solution	8.6.8Incident Management tool a)The solution should be able to register any security event and generate trouble ticket. b)The solution should provide complete life cycle management (workflow) of trouble tickets from incident generation till closure of the incident. c)The solution should provide the logging facility to different levels of users to monitor and manage the incidents generated for closure of the same as per the defined workflow. d)The proposed solution should be able to integrate all the security devices/solutions being proposed as a part of the current RFP/existing and future security devices and solutions identified by the bank. e)The Incident management should include escalation as per the escalation matrix. f)The solution should be able to send the incident report vide email and report submission notification vide SMS.	Bidder request to clarify whether the existing Ticket Management can be leveraged. Also, check & confirm if OEM hosted SaaS Model deployment will be inline with the Banking Compliance & Regulatory recommendations. If both the options are not acceptable then on-premise Ticket Management Solution (EMS Solution) will be the only probable solution which will increase the TCO for project.	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total on-prem SIEM solution.
91	Page No.18	8.6.8 Incident Management tool	Security Information & Event Management (SIEM) - Incident Management tool	"d. The proposed solution should be able to integrate all the security devices/solutions being proposed as a part of the current RFP/existing security devices and solutions identified by the bank." Will there be any additional security devices to be integrated apart from the listed devices in table 26 kindly clarify ? if yes then share the additional list ? "f. The solution should be able to send the incident report in various forms like e-mail, SMS etc." For e-mail integration will bank provide their existing e-mail server for integration and for SMS who will pay the per SMS cost since this is a reccuring component and what is the expected number of SMS per month or year - kindly clarify ?	Please refer to Annexure-7 for detailed scope of work. In future, Bank may request the selected bidder to integrate the additional system/applications. The bidder may use the existing e-mail & SMS services for integration.
92	Page No.19	8.9.3 Vulnerability Management Services	Vulnerability Management Services	Please clarify whether Bidder can propose the VMS as a Service model instead of dedicated on-premise VMS Solution deployment	Only On-Prem solution is expected to be provided.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
93	Page No.31	Clause 24.3	Operations Phase - The minimum number of resources to be provided are 6 - L1, 2 - L2 and 1 - L3.	Requesting KGB to increase the on-site resource count as SOC has to maintain on 24X7 basis. As per theminimum asked by the RFP which is tough to maintain all critical technologies. Would request to consider the resource count as 10 L1, 4 L2 & 2 L3.	Those are the minimum no of resources, it is upto to bidder to deploy competitive resources in order to meet the stated SIEM SLAs and drive the operation smoothly.
94	Page No.31	Clause 25	Service Level Agreements	Requesting the Bank to modify the penalty cap from 10% to 5%	Bidder to comply with RFP Terms.
95	Page No.33	Table – 7 Service levels during SOC operations	All Critical, High, and Medium priority events should be logged as per below SLAs: Events along with action plan/ mitigation steps should be alerted to designated bank personnel as per the below SLA: •Critical events within 15 minutes of the event identification. Update should be provided every 15 minutes till the closure of the incident •High priority events within 30 minutes of the event identification. Update should be provided every 1 hour till the closure of the incident. •Medium priority events within 60 minutes of the event identification. Update should be provided every 4 hours till the closure of the incident. SLA is measured on a monthly basis and the penalty is as follows: **Critical Events** •95-99%: 10% of the Monthly CSOC Resource	Bidder request to amend the clause that " Only automated Event Response Management for same SLA measurement purposes will be considered. Manual Event Response will not be considered as part of Event Response SLA measurement; if any."	Bidder to comply with RFP Terms.
96	Page No.33	Table – 7 Service levels during SOC operations	The SI is expected to perform and provide Vulnerability Assessment Reports with remediation steps. Post Closure of the Identified Vulnerabilities SI is needed to perform a re-assessment of the identified devices. An incident needs to be logged forall vulnerabilities identified, and the incident response SLA shall apply for these.	Bidder request to clearly that what will be the qualification Criteria of identified vulnerabilities to log them as an incident under critical, High, Medium, Low categories and how the each & every vulnerability will get qualify for a Security Incident.	Bidder needs to work in collaboration with the Bank security team, to categorize the incidents as defined in Table 7 (a) of RFP.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
97	Page No.34		The timelines required for resolution of Critical, High, and Medium priority mentioned below: •Critical incidents within 60 minutes of the event identification. Update should be provided every 15 minutes till the closure of the incident •High priority incidents within 90 minutes of the event identification. Update should be provided every 1 hour till the closure of the incident. •Medium priority incidents within 120 minutes of the event identification. Update should be provided every 4 hours till the closure of the incident. The required success rates for the incident resolution are outlined below: **Critical Incidents** •90-95%: 10% of the Monthly CSOC Resource Cost •85 to less than 90%: 15% of the Monthly CSOC Resource Cost •85%: 20% of the Monthly CSOC Resource Cost	Bidder request to amend the clause as "Bidder shall propose the SOAR platform to meet the RFP Event resolution SLA requirement. Manual resolution of Security incidents will not be considered as part of the SLA measurement."	Bidder to comply with RFP Terms.
98	Page No.36	Table – 7 Service levels during SOC operations	Continual Improvement •Quarterly reports need to be provided by the 5th day of each quarter beginning. •Delay in providing quarterly reports shall lead to 1 % of the Quarterly SOC resource cost. •Reduction by 2% in the time for event response, quarter on quarter.	Bidder request to remove the clause of "reduction by 2% in the time for event response, quarter on quarter." Already, Bank does have the penalty clause against event response SLA which is very stringent to get compliant. If Bank is also looking forward for the reduction in event response then associated response SLA penalty shall be removed."	Bidder to comply with RFP Terms.
99	Page No.37	25.2 Penalties/Liquidated damages for not maintaining uptime during operational phase would be as under:	Table: 7 (a) Event Classification	Bidder request to remove the Service Availability, App, Web, DB etc. related problems, issues, Events statements to qualify as Security Incident considerations. Its highly recommended to revise the Security Incident qualification and categorization criteria which shall be related to Security incidents/breaches only.	Bidder to comply with RFP Terms.
100	Page No.80	Table 21:Resource Matrix - L1, L2,L3	Engineer (BE / B. Tech/MCA) CCNA/CCSP/ any SIEM technical certification	Requesting KGB to include BSC-IT /BCA as Education Qualification and Also include CEH as Skill Certification for L1 as well.	Refer Amendment No.1.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
101	Page No.82	Annexure-7 Scope of Work	Along with the SOC operations the SI need to manage and maintain day to day business operation for PIM, Anti-APT and Vulnerability management and scanner.	Kindly confirm if bidder can consider Additional resources as required for the following Services as monitoring of CSOC and managing the specific solutions are two different areas.	Bidder to comply with RFP Terms.
102	Page No.83	Table 23	Existing Infrastructure to be integrated with SIEM:	Kindly share details scope of work for integration with the existing infrastructure	Please refer to Annexure-7 for detailed scope of work.
103	Page No.83	Table. 24 and Table. 25	Log collectors to be deployed at two locations i.e. DC and DR	Please confirm	Refer Annexure 4 & Table-23 for further details.
104	Page No.84	Sizing	The expected EPS count for the bank should be minimum of 10000 and scalable to 30000.	Does the server for the SIEM support 30K EPS on the day one or do we need to privide it for 10K on Day one and provide a roadmap on scalability. Please clarify.	The bidder needs to provide hardware capable for 30000 EPS from day 1. Please refer Annexure-7 Scope of Work (Sizing) for EPS licenses.
105	Page No.1, Annexure-2 Technical Requirements-SIEM	Point No. 5	The proposed solution must ensure all the system components continue to operate when any other part of the system fails or loses connectivity.	Request Bank to confirm does Solution to be considered in all Layer with HA at both DC & DR, kinldy elobrate the requirment	Please refer to Annexure-7 of the RFP for more details.
106	Page No.2, Annexure-2 Technical Requirements-SIEM	Point No. 11	The proposed solution should have connectors to support the listed devices/ applications, wherever required the vendor should develop customized connectors at no extra cost	The cusom connectors could be built by bidder / provider. Request Bank to modify as appropriate.	Please refer Amendment No.1.
107	Page No.3, Annexure-2 Technical Requirements-SIEM	Point No. 18	The proposed solution shall allow bandwidth management, rate limiting, at the log collector level.	SIEM solutions are expected to work on real time information and correlation on real time data ingested. Any deviation in these requirement would impact the overall threat detection and reponse. Thus requesting to realx this clause	The stated requirment is preferrential in nature not an essential one.
108	Page No.3, Annexure-2 Technical Requirements-SIEM	Point No. 24	Traceability of logs shall be maintained from the date of generation to the date of purging.	Request Bank to confirm log retention period for online, offline and archival time frame.	Please refer to section 8.6.6 (a) & table-1 of the RFP for more details.
109	Page No.3, Annexure-2 Technical Requirements-SIEM	Point No. 27	The proposed solution should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.	Request bank to elobrate the requirment, does this request to address for Anlytical purpose or for incident management purpose	Bank require raw logs for incident analysis and forensics purposes as per the regulatory requirements.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
110	Page No.3, Annexure-2 Technical Requirements-SIEM	Point No. 28	The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	This clause is a repeat of clause 9. Request deletion of duplicate clause.	Bidder to comply with RFP Terms.
111	Page No.4, Annexure-2 Technical Requirements-SIEM	Point No. 32	The proposed solution should be able to integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating events. These data feeds should be updated automatically by the proposed solution.	Will the security and threat intelligence feeds data be provided by Customer or the threat intelligence feeds has to be bundled as part of the solution proposed? Are you looking for only Threat Intelligence Feeds or Platform to aggregate all the TI Feeds which will help you to provide better correlation.	The Threat intelligence feeds has to be bundled as part of the proposed solution. In order to detect threats accurately, and threat feeds can be correlated with network activity to spot suspicious activities, threats, and/or exploits.
112	Page No.6, Annexure-2 Technical Requirements-SIEM	Point No. 49	The proposed solution should provide event playback for forensic analysis.	Request to relax	The mentioned requirement is preferrable in nature rather an essential requirement.
113	Page No.6, Annexure-2 Technical Requirements-SIEM	Point No. 49	The proposed solution should provide event playback for forensic analysis	Request to amend this clause as "Proposed SIEM solution should have OOB integration with Packet Capture tool" (clause No.49 is OEM specific)	The bidder is required to propose the solution in order to fulfill the requirement even if an OOB integration is required.Bidder to comply with the RFP terms.
114	Page No.7, Annexure-2 Technical Requirements-SIEM	Point No. 62	Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard.	Request to amend this clause as "Administrators should be able to view correlated events, normalized event details, real-time raw logs and historical events through the dashboard."	Bidder to comply with RFP Terms.
115	Page No.7, Annexure-2 Technical Requirements-SIEM	Point No. 68	The proposed solution should be possible to automatically create incidents and track their closure	This is a vendor specific spec, please remove or modify as " The proposed solution should manage the workflow and the service provider team has to track it till closure.	Please refer Amendment No 1.
116	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 70	Pre-defined parsers are available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	SIEM comes with the multiple Out of box parsers, if a specific parser is not available for any device / application, bidder would be able to create a custom parser. Please remove this spec or modify to accommodate all parsers which are required in the scope of work.	Please refer Amendment No 1.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
117	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 70	Pre-defined parsers are available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	Kindly modify this clause to include solution's capability to create parser for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	Please refer Amendment No 1.
118	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 70	Pre-defined parsers are available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	Request to amend as "Proposed solutino should have OOB parsers or customer parser creation with efforts consideration should be available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)"	Please refer Amendment No 1.
119	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 71	The proposed solution should be able to conduct full packet capture and securely store these packets for a minimum of 30 days	Request to amend as " Proposed SIEM too should have OOB integration with full Packet capture tool"	In order to meet the requirement the bidder can suggest an OOB with full packet capture as part of an overall SIEM solution.
120	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 72	The proposed solution should be able to intercept and review the SSL/TLS encrypted packets.	We understand Bank had asked for a SSL decryptor in the Commercial and Technical Bill of Material and this spec is related to SSL Decryptor not on the SIEM itself. Please confirm. Different OEMs addresses the SSL traffic decryption requirement in a different way, some may use software decryptor while others use a dedicated SSL decryptor so that the load on the SIEM / PCAP would be reduced (SSL traffic) to focus more on the Security Analytics / monitoring. We request Bank to modify the spec if it is related to SIEM to SSL Decryptor.	SPEC is related to SSL decryptor. We are envisaging SSL decryptor as a part of SIEM Solution. Plese Refer Annexure-4 of RFP.
121	Page No.8, Annexure-2 Technical Requirements-SIEM	Point No. 77	The proposed solution should offer a means of escalating alerts between various users of the proposed solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.	Feature of ITSM tool	Bidder to comply with RFP Terms.
122	Page No.9, Annexure-2 Technical Requirements-SIEM	Point No. 84	The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin	Please provide clarity	As part of the overall proposed SIEM solution along with Tier 1 and Tier II storage requirements, Bank should be capable to analyse the incident logs from their inception with respect to time, the related logs and from where these incident logs have originated from.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
123	Page No.9, Annexure-2 Technical Requirements-SIEM	Point No. 86	The proposed system should have capacity to maintain the logs for 90 days on box and 1-year logs on Tier I storage and 5 year logs should be archived on Tier II storage	Kinldy confirm does Bank provides the storage or Bidder should consider the stroge for SIEM Solution.	The bidder should provide the storage for SIEM solution.
124	Page No.9, Annexure-2 Technical Requirements-SIEM	Point No. 85	The storage solution should have the capability to encrypt/hash the logs in storage	For Software solution please allow third party encrytption solution on storage	Bidder to comply with RFP Terms.
125	Page No.10, Annexure-2 Technical Requirements-SIEM	Point No. 99	The proposed solution should be able to Integrate with helpdesk/ ticketing tools	Request bank to confirm existing ticketing too details.	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total SIEM solution.
126	Page No.10, Annexure-2 Technical Requirements-SIEM	Point No. 100	The proposed solution Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	Which solution is Bank using as it's existing backup solution?	Bank's existing backup solution is VEEAM.
127	Page No.10, Annexure-2 Technical Requirements-SIEM	Point No. 100	The proposed solution Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	Please share details of exiting backup solution	Bank's existing backup solution is VEEAM.
128	Page No.10, Annexure-2 Technical Requirements-SIEM	Point No. 100	The proposed solution Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	SIEM is security software and normally not allowed to install any third party softwares, request Bank to remove this clause / modify Solution should come with its own Backup & Restore utility for regular backup and restore.	Bidder to comply with RFP Terms.
129	Page No.10, Annexure-2 Technical Requirements-SIEM	Point No. 100	The proposed solution Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	Request bank to confirm existing Back up tool details Product, Vendors and version details.	Bank's existing backup solution is VEEAM.
130	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 107	The proposed solution should have high availability feature built in. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	Kindly modify this clause to include proposed solution and it's deployment mode/approach should account for high availability feature requested. There should be an automated switch over to secondary collector in case of failure on the primary collector. No performance degradation is permissible even in case of collector failure.	Bidder to comply with RFP Terms.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
131	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 109	The proposed solution should be scalable as per bank roadmap for expansion	Request bank confirm on overall EPS estimated SIEM solution for next 3 years Roadmap to arrive the HW prerequisites accordingly.	Please refer to Annexure-7 for details.
132	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 113	The proposed solution should be preferably appliance-based solution	This clause conflcits with and is a repeat of clause 1. Request deletion of conflicting duplicate clause.	The recommended solution by the bidder can be software based or hardware based.In Annexure 2, specification no 1 is essential in nature whereas specification no 113 is preferable in nature.
133	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 113	The proposed solution should be preferably appliance-based solution	Request to relax	The recommended solution by the bidder can be software based or hardware based.In Annexure 2, specification no 1 is essential in nature whereas specification no 113 is preferable in nature.
134	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 113	The proposed solution should be preferably appliance-based solution	While we support all platforms that is software, appliance, virtual platforms, cloud, please let us know what is required to offer are appliance from OEM to be considered or software with servers? The Specification 1 asks for appliance or software, this spec looks to be conflicting. Please clarify.	The recommended solution by the bidder can be software based or hardware based.In Annexure 2, specification no 1 is essential in nature whereas specification no 113 is preferable in nature.
135	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 114	The proposed solution should be capable of STIX and TAXII bi directionally and should be capable to integrate and auto configure Bank's applicable devices at no cost to the Bank	This clause is a repeat of clauses 32, 36 & 109. Request deletion of duplicate clause.	As a preferable feature it is expected that the recommended solution should be capable of ingesting and transmitting threat intelligence feeds using STIX and TAXII format and protocol.
136	Page No.11, Annexure-2 Technical Requirements-SIEM	Point No. 114	The proposed solution should be capable of STIX and TAXII bi directionally and should be capable to integrate and auto configure Bank's applicable devices at no cost to the Bank	What is expected here? If the expectation is to upload the insights of SIEM to other devices through STIX / TAXII feeds, normally that is not done on any SIEM. Request Bank to remove this spec.	As a preferable feature it is expected that the recommended solution should be capable of ingesting and transmitting threat intelligence feeds using STIX and TAXII format and protocol.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
137	Page No. 13, Annexure-2 Technical requirement-PIM	Point No. 16	The proposed solution should be able to develop privileged identity management audit reports (but not limited to): PCI DSS, RBI guidelines, NABARD regulations , Cert-In, NCIIPC and others.	Requesting you to please rephrase to "The proposed solution should be able to develop privileged identity management audit & compliance reports	Bidder to comply with RFP Terms.
138	Page No. 13, Annexure-2 Technical requirement-PIM	Point No. 19	The proposed solution should support for database-maintained change log for event triggered updates	With database maintaned change log, does it mean capturing change logs of the PAM database? This point is not very clear. Request bank to please elaborate the use case from PAM Integration stand point.	Along with event triggered updates, any changes in the event logs should also be monitored and maintained.
139	Page No. 13, Annexure-2 Technical requirement-PIM	Point No. 20	The proposed solution should have template-based workflows for user account creation, management, group assignments, de-activation and deletion	Request Bank to suggest if they have any existing Identity Management system in place which is used for User provisioning, management and AD group assignments?	Currently Bank is not using any Identity Management System.
140	Page No. 14, Annexure-2 Technical requirement-PIM	Point No. 26	The proposed system should support integration with external GRC, SIEM and HRMS	Request Bank to confirm if the integration is required to support privileged access to GRC, SIEM and HRMS?	The proposed solution should be able to integrate with SIEM & HRMS. In future if Bank procures GRC solution the same needs to be integrated with PIM solution.
141	Page No. 14, Annexure-2 Technical requirement-PIM	Point No. 28	The proposed solution should support for password push to selectable target systems (i.e., the user or administrator is allowed to specify which systems have the same password	Password Push is good but keeping the same password for system is not a good security practice. Request Bank to revisit the requirement and change the "Same Password" clause.	Bidder to comply with RFP Terms.
142	Page No. 14, Annexure-2 Technical requirement-PIM	Point No. 28	The proposed solution should support for password push to selectable target systems (i.e., the user or administrator is allowed to specify which systems have the same password	Please remove this. Same password on multiple system is defeating the PIM solution requirement	Bidder to comply with RFP Terms.
143	Page No. 17, Annexure-2 Technical Requirements- Anti-APT	Point No. 3	The solution should be able to identify and prevent malware present in file types and web objects such as (QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll,ico, jar, jpeg, jpg, mov, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc.) and be able to quarantine them.	Should the sandbox scan the following file types as well:: 7z,cab,csv,doc,docm,docx,dot,dotm,dotx,exe,jar,pdf,potx,pps,ppsm,ppsx,ppt,pptm,pptx,rar,rtf,scr,swf,tar,xla,xls,xlsb,xlsm,xlsx,xlt,xltm,xltx,xlw,zip,pif,com,gz,bz2,tgz,apk (android),ipa (iphone),ISO,js,cpl,vbs,jse,vba,vbe,wsf,wsh	Apart from the mentioned, if the propose solution is able to scan more file types the bidder may propose the respective solution.
144	Page No. 17, Annexure-2 Technical Requirements- Anti-APT	Point No. 5	The solution should support on premise Sandbox test environment which can analyze threats to various operating systems, browsers, desktop applications and plug-ins etc.	Does the bank require on-prem sandbox from day-one? If so, what is the expected 'files per hour'?	The solution has to be on-prem from day 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
145	Page No. 17, Annexure-2 Technical Requirements- Anti-APT	Point No. 8	The solution should be appliance based with hardened OS. No information should be sent to third party system for analysis of malware automatically. It is expected that the solution will send only hash values to anti-virus vendors to get signatures if the signatures are not available. It is expected that all analysis of malware will happen onsite in sandbox environment.	Considering this specification is preferential can a VM based solution be positioned?	It is up to the bidder to meet the mentioned requirements and propose the solution accordingly.
146	Page No. 18, Annexure-2 Technical Requirements- Anti-APT	Point No. 9	The solution should be able to block the call back tunnel including fast flux connections.	Additionally, the solution should be able to reverse engineer malware in order to uncover their DGA (Domain Name Generation) algorithm and identify all their dynamic domain names. Refer to https://en.wikipedia.org/wiki/Domain_generation_algorithm	The bidder may provide additional features apart from the mentioned requirements within the RFP.
147	Page No. 18, Annexure-2 Technical Requirements- Anti-APT	Point No. 10	The solution should be able to integrate with deployed appliances to share malware information/ zero-day attacks knowledge base.	Please specify which deployed appliances it is supposed to share the malware information with, i.e. firewalls, proxy etc.. Also please mention the OEM of the appliances	The proposed Anti-APT solution to be integrated with the proposed SIEM solution.The details of OEM will be shared with the selected bidder.
148	Page No. 19, Annexure-2 Technical Requirements-VM	Point No. 1	The proposed solution should have minimal impact on traffic, server performance, networks etc. during deployment and operation	What is the minimial impact raio or parameter . Please clarify?	Minimal impact means, while running VM scan in the production environment there should not be any significant impact on other applications.
149	Page No. 19, Annexure-2 Technical Requirements-VM	Point No. 4	The proposed solution should provide pre-built integrations with other security solutions	Please mention the integration of security solutions which Bank needs	Please refer to section-8 and Annexure-7 of the RFP.
150	Page No. 19, Annexure-2 Technical Requirements-VM	Point No. 6	The proposed solution should support application scanning, endpoints (laptops or desktops) scanning	Application scanning please clarfiy internal or external?	Bank will utilize the VM tool for scanning both external and internal facing applications.
151	Page No. 19, Annexure-2 Technical Requirements-VM	Point No. 6	The proposed solution should support application scanning, endpoints (laptops or desktops) scanning	Please provide the definition of the word "application" in the clause. Is it referred to as " application software installed on the system" or as " web-application".	Applicationn scanning includes Application softwares installed on the system and Web applications.
152	Page No. 20, Annexure-2 Technical Requirements-VM	Point No. 18	The proposed solution should be able to scan application databases for vulnerabilities	Please share the database lists as to ensure compatability.	Bank will share the database OEMs to the selected bidder.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
153	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 32	The proposed solution should be able to track the closure of all vulnerabilities identified and should include parameters such as responsible person, date of closure, action taken etc.	This is can be achieved integrating ITSM solution.Request you to kindly let us know what ITSM solution Bank is using	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total SIEM solution.
154	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 34	The proposed solution should be able to integrate with other security solutions (i.e. SIEM, Patch Management etc.)	Please share the vendor names of the solutions mentioned to integrate	Bidder to comply with the RFP terms and details will be shared with the selected bidder.
155	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 34	The proposed solution should be able to integrate with other security solutions (i.e. SIEM, Patch Management etc.)	1. Requesting bank to provide the OEM details of the existing SIEM/patch-management solutions. 2. Also requesting bank to confirm on the scope and level of integration expected. 3. Rapid7's vulnerability management solution supports open APIs. These APIs can be used by 3rd party OEMs for integration Rapid7's vulnerability management solution with their respective solutions.	1. The Proposed VM solution should be able to integrate with the propsed SIEM solution. 2. Please refer to Annexure-7 for more details.
156	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 36	The proposed solution should integrate with the existing/ proposed WAF solution	Pleae share the use case for the integration on WAF and mention the vendor name for WAF	Bank will share WAF & use cases with the selected bidder.
157	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 36	The proposed solution should integrate with the existing/ proposed WAF solution	This specific ask is not applicable to VA Solution Offering. Request you to remove this.	Bidder to comply with RFP Terms.
158	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 36	The proposed solution should integrate with the existing/ proposed WAF solution	Please provide the use-case of integrating infrastructure vulnerability scanning solution with the WAF solution? WAF solutions are integrated with the web-application-vulnerability-scanning solutions, so is there an ask for web-application-vulnerability-scanning solution too? If yes, then the requiement is for how many web-applications?	Bank will provide WAF & use case details to the selected bidder.
159	Page No. 21, Annexure-2 Technical Requirements-VM	Point No. 37	The proposed solution should support integration with threat feeds, allowing vulnerabilities to be correlated against real-time threat information.	Pleae share the use case for the integration on TI platform and mention the vendor name for WAF	Bank will provide WAF & use case details to the selected bidder.
160	Page No. 22, Annexure-2 Technical Requirements-VM	Point No. 47	The proposed solution should integrate with asset management systems available in the network.	Please share the vendor for asset managenent tool and the use case	Bank will provide vendor name & use case details to the selected bidder.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
161	Page No. 22, Annexure-2 Technical Requirements-VM	Point No. 47	The proposed solution should integrate with asset management systems available in the network.	1. Requesting bank to provide the OEM details of the existing asset management system. 2. Also requesting bank to confirm on the scope and level of integration expected. 3. Rapid7's vulnerability management solution supports open APIs. These APIs can be used by 3rd party OEMs for integration Rapid7's vulnerability management solution with their respective solutions.	1. The Proposed SIEM solution should be able to integrate with the propsed VM solution. 2. Please refer to Annexure-7 for more details.
162	Page No. 23, Annexure 2 - Other General requirements	Point No. 4	Any changes to the solutions deployed should be logged including changes to database such as Update, insert, delete, select etc. (DML), Schema/Object changes (DDL), Manipulation of accounts, roles and privileges (DCL), Query updates.	Does the ability to log activities and using logs for troubleshooting meet the requirement, even though its not in the form of DML, DDL, DCL? Information includes accessed, authentication, system & application events, memory usage, engine communications, logs on database, and user related configuration changes events.	The proposed solution should be able to log any changes with respect to databases.
163	Page No. 23, Annexure 2 - Other General requirements	Point No. 8	All devices should comply with FIPS-140-2 standard for cryptographic modules	Need more clarifications	The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating that the cryptographic modules meet well-defined security standards.
164	Page No. 23, Annexure 2 - Other General requirements	Point No. 8	All devices should comply with FIPS-140-2 standard for cryptographic modules	Assuming here devices means hardware appliances to be comply with FIPS 140-2 standard for cryptographic modules. Software solutions are exempted from this clause. Please confirm if the understanding is correct.	FIPS-140-2 standard for cryptographic modules only for hardware appliances.
165	Page No. 24, Annexure 2 - Other General requirements	Point No. 17	The bidder should provide continuous threat updates from sources such as CERT, ISAC, NIST, RBI etc.	TIF from Government sources (i.e. CERT, ISAC, NIST, RBI etc.) will be provided by Bank .The same will be integrated with SIEM platform. Kindly confirm if the undestanding is correct	Bidder to provide threat feeds from available resources and integrate with the SIEM. Threat feeds from CERT & RBI will be provided by the Bank.

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
166	Annexure 4, Page No.1	SIEM Product Details	SSL Decryptor	What is the total throughput requirement? 2. What is the SSL throughput requirement? 3. What is the SSL TPS count? 4. Please specify the port requirement. 5. What is the growth expectation for next 6 years	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. * Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps * Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% * Volume of SSL transactions : 30% * Bank is currently using standard Ciphers which supports TLS 1.2 and above.
167	Annexure 4, Page No.1	SIEM Product Details	SSL Decrypter	For SSL Decrypter, please share below asked information: 1. What is the SSL Decrypter hardware throughput requirement? 2. What is the SSL throughput requirement? 3. What is the SSL TPS count? 4. Please specify the port requirement.	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. * Bank Internet Throughput a. DC: 100 Mbps b. DR: 100 Mbps * Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% * Volume of SSL transactions : 30% * Bank is currently using standard Ciphers which supports TLS 1.2 and above.
168				Monthly log volume is 30,000 EPS Please confirm	30,000 EPS is the growth projection for 6th year.

Response to Pre-bid Queries RFP ref: KaGB:Project Office : 03/2021-22 dated 07.02.2022

Sr No	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Bank's Reply
169	NA	NA	Additional clarification for Anti-APT	The Anti-APT solution should be able to fingerprint applications and websites and provide weekly or monthly statistics on user bandwidth usage; based on categories	Bidder to comply with RFP Terms.
170	NA	NA	Additional clarification for Anti-APT	Application control database must contain more than 6000 known applications.	Bidder to comply with RFP Terms.
171	NA	NA	Additional clarification for Anti-APT	The solution should have mechanisms to protect against spear phishing attacks	Bidder to comply with RFP Terms.
172			General	Bidder request to increase the IP count for 512 with 3 years Subscription for VMS OEM participation.	Bidder to comply with RFP Terms.