Response to pre-Bid Queries wrt RFP ref: KaGB:Project Office:RFP:02/2021-22 dated 18.10.2021					
Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
1	2	Bid Details in Brief, Sr. No. - 12	Application Fees (Non Refundable) - INR 59,000 Inclusive of GST @ 18%	Kindly Please allow exemption of Application fees for registered MSME and start-ups as per Central Procurement Policy (CPP) - Government of India	Please refer clause No.40
2	13	6. Participation Methodology	6.1 In a tender either the partner/distributor/System Integrator on behalf of the OEM/OSD or OEM/OSD itself can bid but both cannot bid simultaneously for the same item/product in the same tender.	This clause is restrictive in nature, kindly delete this clause	Bidder to comply with RFP Terms
3	13	6. Participation Methodology	6.2 If a partner / distributor / System Integrator bids on behalf of the OEM/OSD, the same partner/distributor/System Integrator shall not submit a bid on behalf of another OEM/OSD in the same tender for the same item/product.	This clause is restrictive in nature, kindly delete this clause	Bidder to comply with RFP Terms
4	14	8.2	All the Hardware/Software ordered for Supply, Installation, Implementation, Commissioning, Monitoring and Maintenance of Cyber Security Operations Centre Solution should have comprehensive onsite warranty of 3 years and AMC / ATS Period of 3 Years (if Contracted)	Please confirm if onsite security monitoring is required from warranty period only,or it should be for warranty + AMC period i.e. 3+3 Years	Bidder to comply with RFP Terms
5	14	8. General Scope of Work for each solution	8.3 Bank reserves the right to increase or decrease the quantum of purchase by 25% during the contract period in respect to the quantity specified in this tender at the same rate arrived at on the Terms and Conditions of this tender.	Kindly modify this clause to 8.3 Bank reserves the right to increase or decrease the quantum of purchase by 10% during the contract period in respect to the quantity specified in this tender at the same rate arrived at on the Terms and Conditions of this tender.	Bidder to comply with RFP Terms
6	20	9. General Responsibilities of the Security System Integrator	9.1 Training a) The selected bidder shall arrange OEM / OEM Authorized Partner to provide pre-implementation, post-implementation training as per the below table for 10 people nominated by the bank for each solution.	We understand that training is to be provided in at a central location in bangaluru only, kindly confirm	Yes, Location of the training is Bengaluru. Please refer clause 9.1 (e)
7	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
8	20	9.1 Training	Location of the training must be in Bengaluru.	Request bank to confirm facility management for Training will be provided by bank or bidder needs to do the arrangement.	It is the responsibility of the Selected Bidder
9	20	9.1 Training	h) The bidder is also responsible for conducting annual training to the identified persons in the Banks.	For how many persons and what will the duration of these trainings?	The bidder is responsible for conducting annual training for 5 people nominated by the Banks for a period of 8 days.
10	23	9.9 Period of Contract - a	Bidder is required to provide the services for a period of 6 years	is the total contract duration to be 6 years including implementation or excluding implementation ?	Contract Period is including the implementation period.
11	23	9.9 Period of Contract	c) The Bidder is required to provide the warranty / AMC/ATS services (if Contracted) at Bank's DC / DRC and other locations for which tools are procured or where tools are deployed, directly or through their OEM representatives at all locations of Karnataka Gramin Bank and Kerala Gramin Bank.	We understand that the services to be provided at locations as specified in Annexure – 7 Scope of Work documents only, Kindly confirm	Yes, the services to be provided at locations as specified in Annexure – 7
12	25	13	The eligibility technical and commercial bids should be submitted in "Hard copy" and "Soft Copy" in pen drive. The soft copy to be shared to the bank email id apmgroup@kgbk.in	Request Bank to clarify Bidder should submit the Hard Copy Physically and Softcopy in Pen drive as well as through mail.	Bidder should submit the Hard Copy Physically and Softcopy in Pen drive
13	29	23.2	T denotes the date of acceptance of the Purchase Order by the bidder, for example: T+12 represents that the solution needs to be implemented within 12 weeks of the acceptance of the Purchase Order.	Please confirm if warranty and AMC period is inclusive of Implementation time or Warranty is required to start after the implementation.	Bidder to comply with RFP terms
14	29	23.3 Table 5: Project Timelines	All the in-scope solutions should be implemented parallelly. PIM - T+18 Weeks Anti-APT - T+12 Weeks VM - T+8 Weeks	In current situation hardware delivery is taking 8-10 weeks. Hence, deploying solution within 8-12 weeks from acceptance of PO will be unrealistic. Requesting to please change the timeline of mentioned solutions.	Please refer Amendment No. 1
15	29	23.3 Table 5: Project Timelines	All the in-scope solutions should be implemented parallelly. PIM - T+18 Weeks Anti-APT - T+12 Weeks VM - T+8 Weeks	Considering Covid-19 Pandamic, requesting bank to relax the stringint timeline.	Please refer Amendment No. 1
16	29	23.3	Project Time lines: SIEM-T+24, PIM-T+18, Anti-APT -T+12, VM - T+8, Where T denotes the date of acceptance of the Purchase Order by the bidder	Request Bank to Consider the Project time lines from the date of delivery of Hardware.	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
17	29	23.3	Solution : SIEM,PIM, Anti-APT, VM Timelines (in WeeksT+24,T+18T+12T+8	Considering the volume of the work Bidder request to amend the timeline as per following SolutionSIEMPIMAnti-APTVM Timelines (in Weeks)T+32 T+18T+12T+8	Please refer Amendment No. 1
18	31	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.	Please refer clause 24.3 (b) & 24.3 (c) for more clarity.
19	31	25	Service Level Agreements	Requesting the Bank to limit the penalties to only scope of the solution affected.	Bidder to comply with RFP Terms
20	31	25	Service Level Agreements	Requesting the Bank to modify the penalty cap from 10% to 5%	Bidder to comply with RFP Terms
21	32	Cl. 25.2	The bank has not provided a maximum penalty for Uptime	We request that the maximum penalty paid for not maintaining Uptime during Operational phase be 10% of Annual Uptime Charges	Bidder to comply with RFP Terms
22	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 Amendment No.1
23	33	25.2 - Table – 7	Table – 7 Service levels during SOC operations Penalties	Request Bank to consider the Service levels during SOC operations Penalty cap to 10%	Bidder to comply with RFP terms
24	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
25	33	1	SLA Uptime Penalty: 99.9% and above NA 98% to 99.89% - Penalty 5% 95% to 97.99% - Penaty 8% Below 95% - 15%	Request Bank to amend the clause as below, "SLA Uptime Penalty: 99.9% and above NA 98% to 99.89% - Penalty 5% 95% to 97.99% - Penaty 7% Below 95% - 10%"	Bidder to comply with RFP terms
26	33	Table - 7 Service Levels during SOC Operations - Event Response	SLA - 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 event identification. High Priority - within 30 minutes of event identification. Medium - within 60 minutes of event identification.	We request Bankt to modify the penalties for all SLA to as follows 1. 95%-99% - 2% of monthly CSOC Resource cost 2. 90 to less than 95% - 4% of monthly CSOC Resource Cost 3. <90% - 5% of monthly CSOC Resource Cost Overall penalty capped at 5% of CSOC resource cost.	Bidder to comply with RFP Terms
27	37	Table – 7 Service levels during SOC operations	i) If monthly uptime is less than 95%, the Bank shall levy penalty as above and shall have full right to terminate the contract under this RFP or AMC/ ATS, if contracted. The right of termination shall be in addition to the penalty. The above penalty shall be deducted from any payments due to the bidder (including AMC/ ATS payments).	All penalties viz. Liquidated damages/Termination cost/SLA Penalty shall be capped to maximum of 5% of total contrct value	Bidder to comply with RFP Terms
28	38	25.6	All the Liquidated Damages are independent of each other and are applicable separately and concurrently. GST is applicable on Liquidated damages.	We request Bank to modify this clause and put an overall cap to overall penalty and LD charges.	Bidder to comply with RFP Terms
29	41	30. Evaluation of Bid	The Commercial Bid will comprise of Total Cost of Ownership (TCO). The final selection of the bidder will be on the basis of the Technical Score (T) with 60% weightage and the Total Cost of Ownership (TCO) with 40% weightage.	Request you consider the evaluation on L1 basis after meeting the technical weightage of 60%.	Bidder to comply with RFP Terms
30	44	30.14 Scoring for Past Experience	v. Bidders can submit as many reference letters/PO's showing the experience of in-scope solutions. However, Bank will consider only Five references as mentioned in Annexure-3 for evaluation purpose.	We request you to consider 3 projects reference for the purpose of evaluation and providing maximum marks and make the changes to Annexure 8 accordingly.	Bidder to comply with RFP Terms
31	47	35. Bid Validity Period	The offer submitted and the prices quoted therein shall be valid for 180 days from the date of opening of Commercial Bid. Bid valid for any shorter period shall be rejected by the Bank.	Request you to reduce the bid validity period to 90 days	Bidder to comply with RFP Terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
32	50	Security Deposit / Performance Bank Guarantee	43.4 Security Deposit/Performance Bank Guarantee should be valid for 4 years from the date of acceptance of the purchase order. The guarantee should also contain a claim period of twelve months from the last date of validity.	We request you to kindly gove clarity on exact validity of PBG. As in tender the warranty and AMC mentioned is 3+3 years.	Security Deposit/ Performance Bank Guarantee should be valid for 4 years from the date of acceptance of the purchase order.
33	51	45. Delivery, Installation, Integration and Commissioning	45.2 (a) Supply of Hardware and Software items: Within 6 weeks from the date of acceptance of Purchase Order	Delivery to be changed to 14-16 weeks considering the global shortage of semi conductors	Please refer Amendment No. 1
34	51	45.2	a) Supply of Hardware and Software items: Within 6 weeks from the date of acceptance of Purchase Order b) Installation, Configuration, and Implementation: as per Timelines defined in the Clause no. 23.	Request Bank to amend the Clause as "a) Supply of Hardware and Software items: Within 16 weeks from the date of acceptance of Purchase Order	Please refer Amendment No. 1
35	52	47. Roll Out and Acceptance	Banks will evaluate the proposed Cyber Security Operations Centre solution after the Cyber Security Operations Centre solution has been successfully implemented, if during the implementation period, the Cyber Security Operations Centre solution experiences no failures and functions according to the requirements of the RFP, as determined by the Bank; the Cyber Security Operations Centre solution shall be considered accepted by the Bank and the project will be considered deemed signed-off.	Kindly clarify what is the expected signoff criteria, whether it will be after implementation of each solutions or the entire package.	Bank will provide sign-off for each of the in-scope soltion seperately.
36	53	50.1	For SIEM : 30% on Delivery, 60% on Integration & Implementation, 10% for Warranty BG For PIM: 30% on Delivery, 40% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG For Anti-APT: 30% on Delivery, 40% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG For VM: 30% on Delivery, 40% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG	Request Bank to Amend the Clause as "For SIEM : 60% on Delivery, 30% on Integration & Implementation, 10% for Warranty BG For PIM: 50% on Delivery, 20% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG For Anti-APT: 50% on Delivery, 20% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG For VM: 50% on Delivery, 20% on Implementation, 20% on Signoff and Intergration and 10% for Warranty BG	Please refer Amendment No. 1
37	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, Inplementation and Warranty.	Please refer Amendment No. 1
38	53	50. Payment Terms	50.1 Payment schedule will be as under for each of the in-scope solutions (SIEM, VM, PIM, and Anti-APT) 30% on delivery 60% on install and 10% on submission of BG for warranty on the SIEM Portion	Please amend to industry standard of , 70% on delivery 20% on install and 10% on submission of BG for warranty on the SIEM Portion	Please refer Amendment No. 1
39	53	Payment Terms for SIEM	30% on Delivery ; 60% on Integration and Implementation ; 10% on Warranty	As SIEM licenses are subscription based(12 months term period, renewed every year depending upon the Contract) and its an operational tool, request to release 90% license/subscription fees on delivery , 10 % against BG.	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
40	53	Table 12: Payment Terms for SIEM	Delivery - 30% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Integration and Implementation: 60% - After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	We request bank to amend the clause as under : Delivery - 70% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Integration and Implementation: 20% - After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	Please refer Amendment No. 1
41	53	50. Payment Terms Table 12: Payment Terms for SIEM	Delivery-30% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Requesting KGB to modify the clause as "Delivery-60% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices "	Please refer Amendment No. 1
42	53	50. Payment Terms Table 12: Payment Terms for SIEM	Integration and Implementation 60%: After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work.	Requesting KGB to modify the clause as " Integration and Implementation 30%: After successful installation, configuration, Integration & commissioning of all Hardware & Software items supplied as per Scope of Work. "	Please refer Amendment No. 1
43	53	50	Payment Terms - PIM, Anti APT and VM	Requesting Bank to Modify Payment terms for PIM, Anti APT and VM from 30%, 40%, 20% and 10% to 60%, 20%, 10% and 10% for Delivery, Implementation, Integration and Warranty.	Please refer Amendment No. 1
44	54,55,56	Payment Terms for PIM, Anti-APT, VM	30% on Delivery ; 40% on Implementation ;20% on Sign-Off &Integration ; 10% on Warranty	As these licenses are subscription based(12 months term period, renewed every year depending upon the Contract), request to release 90% license/subscription fees on delivery , 10 % against BG.	Please refer Amendment No. 1
45	53	50. Payment Terms	Percentage of Payment on Delivery 30% After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed.	Request you to change as Percentage of Payment on Delivery 90% After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed.	Please refer Amendment No. 1
46	54	50. Payment Terms	Percentage of Payment on Implementation 40% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.	Percentage of Payment on Implementation 10% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
47	54	Table 13: Payment Terms for PIM	Delivery - 30% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation: 40% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. Sign-Off &Integration:20% - After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	We request bank to amend the clause as under : Delivery - 70% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation, Sign-Off &Integration: 20% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. and After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	Please refer Amendment No. 1
48	54	50. Payment Terms: Table 13: Payment Terms for PIM	Delivery 30% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Requesting KGB to modify the clause as " Delivery 60% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Please refer Amendment No. 1
49	54	50. Payment Terms: Table 13: Payment Terms for PIM	Implementation40% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities	Requesting KGB to modify the clause as "Implementation 20% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities "	Please refer Amendment No. 1
50	54	50. Payment Terms: Table 13: Payment Terms for PIM	Sign-Off &Integration20%: After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement	Requesting KGB to modify the clause as " Sign-Off &Integration 10%: After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement	Please refer Amendment No. 1
51	54,55,56	50. Payment Terms	50.1 Payment schedule will be as under for each of the in-scope solutions (SIEM, VM, PIM, and Anti-APT) 30% on delivery 40% on install, 20% on signoff and 10% on submission of BG for warranty on the PIM Portion	Please amend to industry standard of , 70% on delivery 20% on install and 10% on submission of BG for warranty on the PIM Portion	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
52	54-55	Table 14: Payment Terms for Anti-APT	Delivery - 30% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation: 40% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. Sign-Off &Integration:20% - After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	We request bank to amend the clause as under : Delivery - 70% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation, Sign-Off &Integration: 20% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied and integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	Please refer Amendment No. 1
53	54	50. Payment Terms: Table 14: Payment Terms for Anti-APT	Delivery 30%:After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Requesting KGB to modify the clause as " Delivery 60%:After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices "	Please refer Amendment No. 1
54	55	50. Payment Terms: Table 14: Payment Terms for Anti-APT	Implementation 40%: After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities	Requesting KGB to modify the clause as " Implementation 30%: After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities "	Please refer Amendment No. 1
55	55	50. Payment Terms: Table 14: Payment Terms for Anti-APT	Sign-Off &Integration20% :After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement	Requesting KGB to modify the clause as " Sign-Off &Integration20% :After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement "	Please refer Amendment No. 1
56	53	50. Payment Terms	50.1 Payment schedule will be as under for each of the in-scope solutions (SIEM, VM, PIM, and Anti-APT) 30% on delivery 40% on install, 20% on signoff and 10% on submission of BG for warranty on the Anti APT Portion	Please amend to industry standard of , 70% on delivery 20% on install and 10% on submission of BG for warranty on the Anti APT Portion	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
57	55	Table 15: Payment Terms for VM	Delivery - 30% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation: 40% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. Sign-Off &Integration:20% - After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	We request bank to amend the clause as under : Delivery - 70% - After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. Implementation, Sign-Off &Integration:: 20% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work and demonstration of the capabilities as per Annexure-2 to the extent possible within the bank environment. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied and successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement. Warranty: 10% - After completion of warranty period of three years or on submission of Bank Guarantee (BG) for 10% of the hardware/software cost after releasing 90% payment. Warranty BG should be valid till expiry of Warranty period plus claim period of twelve months.	Please refer Amendment No. 1
58	55	Table 15: Payment Terms for VM	Delivery 30% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Requesting KGB to modify the clause as "Delivery 60% : After complete delivery of all hardware and software and Licenses. Please note that Originals of invoices	Please refer Amendment No. 1
59	55	Table 15: Payment Terms for VM	Implementation40% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work	Requesting KGB to modify the clause as "Implementation 30% After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work	Please refer Amendment No. 1
60	56	Table 15: Payment Terms for VM	Sign-Off &Integration 20% :After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement	Requesting KGB to modify the clause as " Sign-Off &Integration 10% :After successful integration with the SIEM solution and demonstration of relevant use cases as per the bank's requirement."	Please refer Amendment No. 1
61	53	50. Payment Terms	50.1 Payment schedule will be as under for each of the in-scope solutions (SIEM, VM, PIM, and Anti-APT) 30% on delivery 40% on install, 20% on signoff and 10% on submission of BG for warranty on the VM Portion	Please amend to industry standard of , 70% on delivery 20% on install and 10% on submission of BG for warranty on the VM Portion	Please refer Amendment No. 1
62	56	50. Payment Terms	50.2 Payment for the SOC maintenance & resource charges will be paid quarterly in arrears on submission of invoice and other supporting documents including monthly SLA reports signed by Bank Officials to the Security System Integrator from the date of sign-off of the project.	Kindly modify this clause to 50.2 Payment for the SOC maintenance & resource charges will be paid monthly in arrears on submission of invoice and other supporting documents including monthly SLA reports signed by Bank Officials to the Security System Integrator from the date of sign-off of the project.	Bidder to comply with RFP Terms
63	56	50. Payment Terms	50.2 Payment for the SOC maintenance & resource charges will be paid quarterly in arrears on submission of invoice and other supporting documents including monthly SLA reports signed by Bank Officials to the Security System Integrator from the date of sign-off of the project	Please amend to Monthly in arrears	Bidder to comply with RFP Terms
64	57	51. Subcontracting	51.1. During Implementation The bidder is not permitted to subcontract the implementation of in-scope solutions to other organizations. 51.2. During Operations The vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.	Bank to kindly confirm that such consent will not be unduly withheld.	Bidder to comply with RFP Terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
65	57	51. Subcontracting	51.1. During Implementation The bidder is not permitted to subcontract the implementation of in-scope solutions to other organizations. 51.2. During Operations The vendor shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract without the prior written consent of the Bank.	Kindly allow subcontracting	Bidder to comply with RFP Terms
66	57	52. Order Cancellation / Termination of Contract	52.1 The Bank reserves its right to cancel the entire / unexecuted part of the Purchase Order at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions: a) Delay in delivery & project implementation beyond the specified period. b) Serious discrepancies noted in the items delivered. c) Breaches in the terms and conditions of the Order. 52.2 The Bank reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by the Bank on the following circumstances: a) Non submission of acceptance of order within 7 days of order. b) Excessive delay in execution of order placed by the Bank. c) The selected bidder commits a breach of any of the terms and conditions of the bid. d) The selected bidder goes into liquidation voluntarily or otherwise. e) An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid. f) The progress made by the selected bidder is found to be unsatisfactory. g) If deductions on account of liquidated Damages exceeds more than 10% of the total contract price. 52.3 Bank shall serve the notice of termination to the selected bidder at least 30 days prior, of its intention to terminate services during contract period. 52.4 In case the selected bidder fails to deliver the quantity as stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the selected bidder by giving 7 days prior notice to the selected bidder 52.5 After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits and at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled. 52.6 The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract. 52.7 In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Bank Guarantee	Kindly confirm that Bank shall only exercise the option to terminate the contract after 30 days of notice to remedy any performance issues, only if the breach is not remedied. Further such termination shall not affect the rights of the Bidder already accrued.	Bidder to comply with RFP Terms
67	58-61	Cl. 53- Cl. 59	53. Local Support, 54. Software, Drivers and Manuals 55. Warranty 56. Annual Maintenance Contract (AMC) / Annual Technical Support (ATS) 57. Scope Involved During Warranty and AMC/ATS period (if contracted) 58. Spare Parts 59. Mean Time Between Failures (MTBF)	Bank to kindly confirm that warranty, support, AMC/ATS conditions in respect of products/software supplied will be as per the OEM/OSD warranty terms and conditions and Bidder being an authorized reseller, will pass on such warranties "as-is", to the Bank." All implied warranties are hereby specifically excluded. All support, maintenance, upgrades, patch/bug fixes, version upgrade/customizations, preventive maintenance to be provided by the OEM.	Bidder to comply with RFP Terms
68	58	53. Local Support	53.4 The Support should be for an unlimited number of incidents reported to them and provide a practical solution to resolve the issue. The support should be provided in person and to the DRC, over phone, E mail web based, if required. All escalations will be attended / responded-promptly not later than 1 hour of reporting.	We understand that the support services to be provided at locations as specified in Annexure – 7 Scope of Work documents only, Kindly confirm	Yes, the services to be provided at locations as specified in Annexure – 7
69	59	54. Software, Drivers and Manuals	54.1 The selected bidder shall supply along with each item all the related documents, Software Licenses loaded in the Cyber Security Operations Centre Solution without any additional cost. The documents shall be in English. These will include but not restricted to User Manual, C-SOC Operation Manuals, Other Software and Drivers etc	Bidder will provide all documents received from OEMs	Bidder to comply with RFP Terms
70	60	56. Annual Maintenance Contract (AMC) / Annual Technical Support (ATS)	56.3 The Bank will pay AMC/ATS charges for Servers (including OS) and Other Items quarterly in arrears after satisfactory completion of service during the period and submission of reports and invoices.	Requesting KGB to modify the clause as " 56.3 The Bank will pay AMC/ATS charges for Servers (including OS) and Other Items Yearly in advance after satisfactory completion of service during the period and submission of reports and invoices	Bidder to comply with RFP Terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
71	60	56. Annual Maintenance Contract (AMC) / Annual Technical Support (ATS)	56.5 It may be noted that the Bank reserves the right to demand additional performance Bank Guarantee to the tune of 10% of the value of the Purchase Order, if AMC/ATS charges quoted by the selected bidder are abnormally low (below 8% of the cost).	Requesting KGB to modify the clause as "56.5 It may be noted that the Bank reserves the right to demand additional performance Bank Guarantee to the tune of 10% of the value of the Purchase Order, if AMC/ATS charges quoted by the selected bidder are abnormally low (below 4% of the cost). "	Bidder to comply with RFP Terms
72	61	57. Scope Involved During Warranty and AMC/ATS period (if contracted)	57.4. The support shall be given in person only.	Request you to modify this to 57.4. The support shall be given in as per SLA requirement.	Bidder to comply with RFP Terms
73	61	57. Scope Involved During Warranty and AMC/ATS period (if contracted)	57.5. Only licensed copies of software shall be supplied and ported in the Servers, Storage Systems, and other Items. The selected bidder shall grant an irrevocable perpetual license to the Bank to use the software. Further, all software supplied shall be of latest version.	Bidder will provide licenses as per the OEMs licensing policy.	Bidder to comply with RFP Terms
74	61	60. Defect Liability	In case any of the supplies and equipment delivered under the Contract are found to be defective as to material and workmanship and / or not in accordance with the requirement, and/or do not achieve the guaranteed performance as specified herein, within the warranty and AMC/ATS period (if contracted) of the contract, the selected bidder shall forthwith replace/make good such defective supplies at no extra cost to the bank without prejudice to other remedies as may be available to the bank as per RFP terms.	All warranty/replacements is as per OEM warranty terms & conditions only. Kindly delete the same.	Bidder to comply with RFP Terms
75	61	60	Support for maintenance of Hardware, software (including OS and software license) and Other Items supplied should be available for a minimum period of 3 years, covering all parts, maintenance, and support, after expiry of warrantyperiod	We offer our services from a Shared Cloud Platform which is hosted in a MeitY approved DC in India. Only the sensors such as scanner and agents need to be deployed in the bank's premises. Hence, we request the bank to accept the subscription to our shared cloud platform	Bidder to comply with RFP Terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
76	62	61. Intellectual Property Rights	61.1 Bidder warrants that the inputs provided shall not infringe upon any third-party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. Bidder warrants that the deliverables shall not infringe upon any third-party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. The bidder should ensure that the Hardware and Software supplied to the Bank shall not infringe the third-party intellectual property rights, if any. The bidder has to ensure that third party rights are not infringed even in case of equipment /software supplied on behalf of consortium as bidder. 61.2 In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, bidder shall at its choice and expense: [a] procure for Bank the right to continue to use such deliverables; (b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; or (c] if the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse bank for any amounts paid to bidder for such deliverables, along with the replacement costs incurred by Bank for procuring an equivalent equipment in addition to the penalties levied by Bank. However, Bank shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the bidder shall be responsible for payment of penalties in case service levels are not met because of inability of the bank to use the proposed solution. 61.3 The indemnification obligation stated in this clause apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims [at the expenses of the indemnifying party]. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby. 61.4 The bidder acknowledges that business logics, workflows, delegation and decision-making processes of Bank are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors of Hardware/Software.	Since we are reseller of products/licenses, hence all third party products/licenses supplied, will be governed by the OEM/Software Licensor terms, and the same shall prevail. We request that provisions related to Indemnity be restricted to Third party indemnification claims arising from infringement of IPR in respect of the Services provided by the Bidder. Further the below limitation of liability clause needs to be included: The cumulative liability of the bidder under the scope of this RFP applicable to the maximum extent allowed in indian laws irrespective of claims under contract, torts or other legal theory is limited to 50% of the charges paid or payable for such Goods and Services under the relevant PO/SOW during the applicable contract year. Neither party shall be liable for indirect, special and consequential loss and damages including but not limited to loss of profit, anticipated savings, loss of data, loss of business.	Bidder to comply with RFP Terms
77	63	63 Indemnity	63.1 The bidder shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities(including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of: a) The breach, default or non-performance of undertakings, warranties, covenants or obligations by the bidder. b) Any contravention or Noncompliance with any applicable laws, regulations, rules, statutory or legal requirements by the bidder; 63.2 The bidder shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of Security Operations Centre Solution supplied by them. a) All indemnities shall survive notwithstanding expiry or termination of the contract and bidder shall continue to be liable under the indemnities. b) The limits specified in the above said clause shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited. c) All employees engaged by the bidder shall be in sole employment of the bidder and the bidder shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall the bank be liable for payment or claim or compensation (including but not limited to compensation on account of injury/ death / termination) of any nature to the employees and personnel of the bidder. 63.3 Bidder's aggregate liability shall be subject to an overall limit of the total Cost of the project.	We request that provisions related to Indemnity be restricted to Third party indemnification claims arising from infringement of IPR in respect of the Services provided by the Bidder. Further the below limitation of liability clause needs to be included: The cumulative liability of the bidder under the scope of this RFP applicable to the maximum extent allowed in indian laws irrespective of claims under contract, torts or other legal theory is limited to 50% of the charges paid or payable for such Goods and Services under the relevant PO/SOW during the applicable contract year. Neither party shall be liable for indirect, special and consequential loss and damages including but not limited to loss of profit, anticipated savings, loss of data, loss of business.	Bidder to comply with RFP Terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
78	64	65. Assignment	65.1 The vendors shall not assign to anyone, in whole or in part, its obligations to perform under the RFP/contract, except with the Bank's prior written consent. 65.2 If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership etc., this RFP/Agreement shall be considered to be assigned to the new entity and such an act shall not affect the rights and obligations of the bank and vendor under this RFP.	Kindly confirm that such consent will not be unduly withheld or delayed. Bidder should also be allowed to assign if bidder undergoes a merger/change of ownership.	Bidder to comply with RFP Terms
79	64	67. Insurance	The Hardware to be supplied will be insured by the bidder against all risks of loss or damages from the date of shipment till such time, the same is delivered and installed at site and handed over to the Bank/Office. The Bidder has to obtain transit insurance cover for the items to be delivered from their factory/godown to the location and such insurance cover should be available till installation of the Cyber Security Operations Centre Solution.	Bank to confirm that the Insurance provided for the Hardware would be transit insurance till the point of delivery.	Bidder to comply with RFP Terms
80	64	68. Guarantees	The bidder should guarantee that the hardware items delivered to the Bank are brand new, including all components. In the case of software, the bidder should guarantee that the software supplied to the Bank are latest version which includes all patches, updates etc., and the same are licensed and legally obtained. All hardware and software must be supplied with their original and complete printed documentation.	Bank to confirm that all hardware & software to be supplied comes with the OEM/Software Licensor guarantee.	Bidder to comply with RFP Terms
81	65	73. Negligence	In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.	Bank to kindly confirm that any cancellation or termination of contract will be done only after giving 30 days written notice to the Bidder to cure or remedy the default and only upon failure of the Bidder to remedy or cure such default.	Bidder to comply with RFP Terms
82	71	Annexure-1 Pre-Qualification Criteria	Annexure-1 Pre-Qualification Criteria	We request you to kindly cosider Credentilas and documents of Parent Company of the Bidding Entity.	Please refer Amendment No. 1
83	71	Annexure-1 Pre-Qualification Criteria	Sl. No. 1 - The Bidder should be a registered company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013, providing information security services for the last three financial years: 2018-2019, 2019-2020 and 2020-2021	Details required for the financial year 2020-2021 is under audit, So we request you to consider the details of FY 2017-2018 and kindly modify the clause as given below. The Bidder should be a registered company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013, providing information security services for the last three financial years: 2017-2018, 2018-2019, 2019-2020.	Please refer Amendment No. 1
84	71	RFP Page No.71 Pre-qualification (PQ) Criteria:	The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2018-2019, 2019-2020 and 2020- 2021.	Humbly requesting Karnataka Gramin Bank to provide relaxation or waivers for Indian based Startups and MSMEs	Please refer Amendment No. 1
85	71	Annexure-1 Pre-Qualification Criteria	Sl. No. 2 - The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2018-2019, 2019-2020 and 2020- 2021.	Details required for the financial year 2020-2021 is under audit, So we request you to consider the details of FY 2017-2018 and kindly modify the clause as given below. The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2017-2018, 2018-2019, 2019-2020.	Please refer Amendment No. 1
86	71	Pre-Qualification Criteria for financial compliance for SI	The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2018-2019, 2019- 2020 and 2020- 2021.	Request to kindly relax the minimum turnover value to INR 5 Crs, considering the business impact during COVID Pandemic.	Please refer Amendment No. 1
87	71	Pre-Qualification Criteria for financial compliance for SI	The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2018-2019, 2019-2020 and 2020- 2021	Request you to consider as"The Bidder's organization should have a Average turnover of INR Twenty Five (25) Crores from information security related services and products for of the past Three (3) financial years: 2018-2019, 2019-2020 and 2020- 2021"	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
88	71	Sr No. 2	The Bidder's organization should have a minimum turnover of INR Thirty (30) Crores per annum from information security related services and products for each of the past Three (3) financial years: 2018-2019, 2019- 2020 and 2020- 2021.	We are a CERT-in empanelled organization and also MSME enlisted. Being a service company, our turnover is low. Would request you to make it average turnover as 2cr per year	Please refer Amendment No. 1
89	71	Annexure-1 Pre-Qualification Criteria for financial compliance for SI, Clause no. 3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India	We request bank to amend the clause as under : The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last five financial years: 2016-17, 2017-18, 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI/Govt. sector in India	Bidder to comply with RFP Terms. Please refer Amendment No. 1
90	71-72	Point 3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions	We request bank to mondified as -The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI / Govt sector in India with the following conditions	Bidder to comply with RFP Terms. Please refer Amendment No. 1
91	71-72	3	Table-16: Pre-Qualification Criteria The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Disclosing customer financial is not possible, neither our customer can provide their financial infrmation. Hence, we request you to remove this 50,000 crore turnover clause.	Please refer Amendment No. 1
92	71-72	RFP Page No. 72 Pre-qualification (PQ) Criteria:	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019- 2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Humbly requesting Karnataka Gramin Bank to provide relaxation or waivers for Indian based Startups and MSMEs	Please refer Amendment No. 1
93	71-72	Pre-Qualification Criteria	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019- 2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021	Requesting KGB to modify the clause as " The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last five financial years:2016-17,2017-18 2018-2019, 2019- 2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores	Please refer Amendment No. 1
94	71-72	3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019- 2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021	Being a Starup India Recognized Company request you to provide an exemption on prior Experience & Turnouver part as per DPIIT.Our DPIIT Registration No-DIPP84301	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
95	71-72	Annexure-1 Pre-Qualification Criteria	Sl. No. 3 - The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Could you please specify which line items to be considered from the annual report to arrive at the business figures.	Please refer Amendment No. 1
96	71-72	Annexure-1, Table-16: Pre-Qualification Criteria for financial compliance for SI, Sr. No. 3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	It is requested to change the criteria as below: "The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any State Government/Central Government/PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Five 5 crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021."	Please refer Amendment No. 1
97	71-72	Pre-Qualification Criteria for financial compliance for SI	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021	Request you to change as "b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR 500 crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021" considering the size and scale of proposed Solution request you to considered 500 crore reference.	Please refer Amendment No. 1
98	71-72	Annexure-1, Table-16: Pre-Qualification Criteria for financial compliance for SI	3. The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the ast three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Request bank to modify the clause as per below: "The bidder/OEM should have executed the SOC OR similar project which includes implementation of proposed SIEM solution OR similar solution during any of the ast three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC OR similar project inclusive of SIEM solution should be minimum of INR Two (2) Crores. b.) The total business of the organization where the SOC OR similar project (Inclusive or exclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021."	Please refer Amendment No. 1
99	71-72	Sl No 3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019- 2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	would request to make single order 1cr and business from SOC can be made 1cr	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
100	71-72	Annexure -1 Point No.3	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Request Bank to Amend the clause as "The bidder should have executed the SOC project which includes implementation of Similar SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1
101	71-72	Pre-Qualification Criteria	The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019- 2020 and 2020-2021 in any PSU/PSB/BFSI sector in India with the following conditions: a.) The TCO of the SOC project inclusive of SIEM solution should be minimum of INR Five (5) Crores. b.) The total business of the organization where the SOC project (Inclusive of SIEM solution) has been implemented should have a minimum business of INR Fifty Thousand (50,000) crore in any of the last three financial years 2018-2019, 2019-2020 and 2020-2021	We requesting you to that kindly change it to as below: The bidder should have executed the SOC project which includes implementation of proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any PSU/PSB/BFSI/ Pvt Banks / Co-Operative Banks Falls Under RBI Guidelines / Government sector in India with the following conditions:	Please refer Amendment No. 1
102	71-72	Annexure-1 Pre-Qualification Criteria	Sl. No. 3 - The bidder's organization should have positive net worth for the last three financial years: 2018-2019, 2019-2020 and 2020-2021 from their Indian operations.	Details required for the financial year 2020-2021 is under audit, So we request you to consider the details of FY 2017-2018 and kindly modify the clause as given below. The bidder's organization should have positive net worth for the last three financial years: 2017-2018, 2018-2019, and 2019-2020 from their Indian operations.	Please refer Amendment No. 1
103	72	Sl No.4	The bidder's organization should have positive net worth for the last three financial years: 2018-2019, 2019-2020 and 2020-2021 from their Indian operations.	Kindly conform on accepting provisional balance sheet for FY2020-21	Please refer Amendment No. 1
104	72	4	Table-16: Pre-Qualification Criteria The bidder's organization should have positive net worth for the last three financial years: 2018-2019, 2019-2020 and 2020-2021 from their Indian operations.	Request you to modify the clause as below: The bidder's organization should have positive net worthin any two of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 from their Indian operations.	Please refer Amendment No. 1
105	72	Pre-Qualification Criteria for financial compliance for SI	The bidder's organization should have positive net worth for the last three financial years: 2018-2019, 2019-2020 and 2020-2021 from their Indian operations.	Request to kindly relax the clause, considering the business impact during COVID Pandemic.	Please refer Amendment No. 1
106	73	Point 1 Category 1	The bidder 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 bank to mondified as-The bidder 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	Please refer Amendment No. 1
107	73	Pre-Qualification Criteria for Technical compliance for SI	The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Request to kindly relax the clause to any ONE PSU/PSB/BFSI, considering the business impact during COVID Pandemic.	Please refer Amendment No. 1
108	73	RFP Page No. 73 Pre-qualification (PQ) Criteria	The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Humbly requesting Karnataka Gramin Bank that can other sector implementation be mentioned	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
109	73	Annexure -1 Table 17. Category I, Point No.b	The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Request Bank to amend the clause as "The bidder should have successfully implemented Similar On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1
110	73	Sl No 1 Point No. b	b.) The bidder should have successfully implemented / managed proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank	We request bank to mondified as b.) The bidder should have successfully implemented / managed proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank/Govt	Please refer Amendment No. 1
111	73	Category 2	The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI / sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	We request bank to mondified as-The bidder should have successfully implemented either On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI / Govt sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1
112	73	Annexure -1 Table 17. note (a)	a.) The Bidder should satisfy of the eligibility criteria for both the category 1 and category 2 solutions.	We request bank to mondified as a.) The Bidder should satisfy either of the eligibility criteria for both the category 1 and category 2 solutions.	Please refer Amendment No. 1
113	73	1	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 - The bidder should have successfully implemented On-Premise AntiAPT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021. Note: a.) The Bidder should satisfy the eligibility criteria for both the category 1 and category 2 solutions. 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.	Being a Starup India Recognized Company request you to provide an exemption on prior Experience & Turnouver part as per DPIIT.Our DPIIT Registration No-DIPP84301	Please refer Amendment No. 1
114	73 & 74	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI, Sr. No. - 1	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	It is requested to change the criteria as below: "Category 1 a.) The bidder should be currently in the service of providing On-Premise Security Operation Centre (SOC) and facility management service for Security solutions in any State Government/Central Government/PSU/PSB/BFSI sector in India b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any one State Government/Central Government/PSU/PSB/BFSI sector in India. Category 2 - The bidder should have successfully implemented On-Premise SIEM/Anti- APT/VM/PIM in any State Government/Central Government/PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021."	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
115	73	Sl No. 1	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021. Note: a.) The Bidder should satisfy the eligibility criteria for both the category 1 and category 2 solutions. 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.	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021. Note: a.) The Bidder should satisfy the eligibility criteria for both the category 1 and category 2 solutions. 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 refer Amendment No. 1
116	73	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI	1. Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021. Note: a.) The Bidder should satisfy the eligibility criteria for both the category 1 and category 2 solutions. 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.	Request bank to modify the clause as per below: "Category 1 a.) The bidder/OEM should be currently in the service of providing On-Premise Security Operation Centre (SOC) OR Similar Solution and facility management service for Security / Fraud OR similar solutions in any PSU/PSB/BFSI sector in India b.) The bidder/OEM should have successfully implemented proposed On-Premise SIEM OR similar solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 The bidder/OEM should have successfully implemented On-Premise Anti- APT, VM, and PIM OR similar solution in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021. Note: a.) The Bidder /OEM should satisfy the eligibility criteria for both the category 1 and category 2 solutions. b.) The Bank will enter into contract with only the bidder & OEM and the responsibility of delivering the project as per SLAs defined in the RFP rests with the bidder/OEM. In case the bidder /OEM showcases the experience of the OEM, the responsibility for implementation shall be still with the bidder/OEM only.	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
117	73 & 74	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI, Sr. No. - 1	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank. Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	We requesting you to that kindly change it to as below: Category 1 a.) The bidder 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/ Pvt Banks / Co-Operative Banks Falls Under RBI Guidelines / Government sector in India b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI / Pvt Banks / Co-Operative Banks Falls Under RBI Guidelines / Government sector in India. Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI / Pvt Banks / Co-Operative Banks Falls Under RBI Guidelines / Government sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1
118	73	Sl No.1	Category 1 a.) The bidder 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 should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Pls allow any PSU , Govt and Enterprise SOC as credentials	Please refer Amendment No. 1
119	73	1	Table-17: Pre-Qualification Criteria Category 1 b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	We are complying almost all part of the qualification, except this clause. We request you amend the clause as below to enable reputaed and qualified bidders to participate: b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI/Government sector in India, out of which one should be a scheduled bank/Government Organization.	Please refer Amendment No. 1
120	72	Table-17: Pre-Qualification Criteria for Technical compliance for SI, Sr. No. 1	Category 1 b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	We request bank to amend the clause as under : The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last Five financial years: 2016-17, 2017-18, 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI/Govt. sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1
121	73	1	Table-17: Pre-Qualification Criteria Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	Though we have experience in implenting these solution, but, we don't have documentary evidence to present here, hence, meeting both the category of expereience is diffcult for us. Request you to put this clause as optional and enable us to bid for this opportunity.	Please refer Amendment No. 1
122	73	Annexure-1 Pre-Qualification Criteria	Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	Request you to kindly consider the projects executedin last five financial years and modify the clause as given below. Category 2 - The bidder should have successfully implemented On-Premise Anti-APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last Five financial years: 2016-2017, 2017-2018, 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
123	73	Table-17: Pre-Qualification Criteria for Technical compliance for SI, Sr. No. 1	Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	We request bank to amend the clause as under : Category 2 - The bidder should have successfully implemented On-Premise Anti- APT, VM, and PIM in any PSU/PSB/BFSI/Govt. sector in India, during any of the last Five financial years: 2016-17, 2017-18, 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1
124	74	2	The bidder's organization should have ISO 27001 certifications.	ISO27001 or ISO 9001	Bidder to comply with RFP Terms.
125	74	The bidder's organization should have ISO 27001 certifications (Point No.2)	Bidder has to submit valid ISO 27001 certification copy	Requesting to amend for ISO 9001	Bidder to comply with RFP Terms.
126	74	Annexure-1 Pre-Qualification Criteria	Sl. No. 2 - The bidder's organization should have ISO 27001 certifications.	request you to modify this clause as follows The bidder's organization/Group Company should have ISO 27001 certifications.	Bidder to comply with RFP Terms.
127	74	RFP Page No.74 Gartner or Forrester report	The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	Humbly requesting Karnataka Gramin Bank to provide relaxation for Indian based Startups and MSMEs. Solutions Proposed by Innspark Solutions are 100% Researched and Developed in India. Not only does InnSpark solution meet every technical and operationsl requirement specified in the RFP, our solution compares winningly with MNC players' solution on many technical, operationsl and economical comparisons.	RFP Clause stands deleted. Please Refer Amendment No.1
128	74	Clause 4	The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	MeiTY issued a notice on March 16, 2021 - No.19-113/2020-SA (https://dot.gov.in/sites/default/files/2021%2003%2016%20PMISec%20Security.pdf) highlighting preference for Make in India cyber security products. This was implemented to promote Make in India products & eliminate restrictions such as Gartner or third party analyst clauses for such products. Gartner or Forrester clauses seem more favourable for international cyber security products. In lieu of this, request the bank to give preference to Make in India cyber security products & relax the Gartner & Forresters clause for the same. Local cyber security product supplier should submit the required Make in India or DIPP certificate as proof.	RFP Clause stands deleted. Please Refer Amendment No.1
129	74	4	The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	Please confirm additional solutions like incident management, SSL decrypter SAN switches has to be considered from Gartner's Leader or challenger magic quadrant or Forrester's wave under Leader or strong performer OEM or can be from any make and model?	RFP Clause stands deleted. Please Refer Amendment No.1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
130	74	4	The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	The solution must a Leader for the last 3 years in Gartner Enterprise Network Firewall, considering it covers all the features mentioned in the specification and there in no other relevant Magic Quadrant for Anti-APT.	RFP Clause stands deleted. Please Refer Amendment No.1
131	74	4	The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	Considering the above facts and Key Government Initiative “MAKE IN INDIA”, we would like to request you to include this in the OEM qualification criteria,therefore allowing a fair chance to Indigenous OEM’s like Netmonastery Network Security Pvt Ltd. (Please find attached the letter from the ministry). Request you to Remove the Gartner Quadrant Clause	RFP Clause stands deleted. Please Refer Amendment No.1
132	74	Table -17: Pre-Qualification Criteria for Technical Complinace for SI (Point 4)	Bidder has to submit Gartner or Forrester report wherever applicable	Gartner or Forrester reprot is for imported product & hence we request consider Make in India product As per Ministry of electronics and information Technology Notification no. 1 (10)/2017-CLES, and do the needful	RFP Clause stands deleted. Please Refer Amendment No.1
133	74	Table -17: Pre-Qualification Criteria for Technical Complinace for SI (Point 4)	Table-17: Pre-Qualification Criteria for Technical compliance for SI : Point No 4 The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	So being an Indian OEM we are requesting you that kindly relax this clause and allow Indian OSD’s / OEM’s to Participate in this RFP as per the Government Of India Guidelines (Make India Initiate).	RFP Clause stands deleted. Please Refer Amendment No.1
134	74	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI	4. The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021.	MeiTY issued a notice on March 16, 2021 - No.19-113/2020-SA (https://dot.gov.in/sites/default/files/2021%2003%2016%20PMISec%20Security.pdf) highlighting preference for Make in India cyber security products. This was implemented to promote Make in India products & eliminate restrictions such as Gartner or third party analyst clauses for such products. Gartner or Forrester clauses seem more favourable for international cyber security products. Conbsidering above, request the bank to give preference to Make in India cyber security products & relax the Gartner & Forresters clause for the same. Local cyber security product supplier should submit the required Make in India or DIPP certificate as proof.	RFP Clause stands deleted. Please Refer Amendment No.1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
135			Additional queries	The solution must a Leader for the last 3 years in Gartner Enterprise Network Firewall, considering it covers all the features metioned in the specification and there in no other relevant Magic Quadrant	RFP Clause stands deleted. Please Refer Amendment No.1
136	74	Sl No.4	"The bidders should ensure all the proposed OEM products (wherever applicable) in the bid for each of the in-scope security solutions should satisfy at least one of the following conditions: i. The product should be in Gartner's Leader or challenger magic quadrant for any of the last three years: 2019, 2020, and 2021. ii. The product should be in Forrester's wave under Leader or strong performer for any of the last three years: 2019, 2020, and 2021. "	We are Partnering India made SIEM Solution and complying the points and we have large number of deployments in India and abroad in all sectors including lot of cooperative and scheduled banks in India and abroad so looking forward to amend the above point/give us a chance as per Make in India solution as per Govt of India directive.	RFP Clause stands deleted. Please Refer Amendment No.1
137	74	Annexure-1 Pre-Qualification Criteria	Sl. No. 5 - The bidder should have a minimum of 5 individuals with prior experience in implementation of SIEM solution out of which a minimum of 3 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.	Request you to modify this clause as follows The bidder should have a minimum of 5 individuals with prior experience in implementation of SIEM solution. The bidders should deploy the experienced resources during implementation at the Bank during the implementation phase.	Bidder to comply with RFP Terms.
138	74	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI, Sr. No. - 5	The bidder should have a minimum of 5 individuals with prior experience in implementation of SIEM solution out of which a minimum of 3 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.	It is requested to change the criteria as below: The bidder should have a minimum of 2 individuals with prior experience in implementation of SIEM solution. The bidders should deploy the experienced resources during implementation at the Bank during the implementation phase."	Bidder to comply with RFP Terms.
139	74	Annexure-1, Table-17: Pre-Qualification Criteria for Technical compliance for SI	5. The bidder should have a minimum of 5 individuals with prior experience in implementation of SIEM solution out of which a minimum of 3 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.	Request bank to modify the clause as per below: "The bidder/OEM should have a minimum of 5 individuals with prior experience in implementation of SIEM solution OR Similar Solution out of which a minimum of 1 individuals should be certified in the proposed solution. The bidders/OEM should deploy the certified and experienced resources during implementation at the Bank during the implementation phase."	Bidder to comply with RFP Terms.
140	75	RFP Page No.75 Pre-qualification (PQ) Criteria	Each of the proposed solutions should have been successfully implemented in a minimum of Two PSU/PSB/BFSI sector in India of which One should be a scheduled bank.	Humbly requesting Karnataka Gramin Bank that can other sector implementation be mentioned	Bidder to comply with RFP Terms.
141	75	Sl No.1	Each of the proposed solutions should have been successfully implemented in a minimum of Two PSU/PSB/BFSI sector in India of which One should be a scheduled bank	For Past Experience the following documents need to be submitted: Copies of reference letter provided by clients where solution is successfully implemented, along with relevant completion certificates. The details are to be submitted as per Annexure-14	Bidder to comply with RFP Terms.
142	75	Annexure-1, Table-18: Pre-Qualification Criteria for Technical compliance for OEMs	1. Each of the proposed solutions should have been successfully implemented in a minimum of Two PSU/PSB/BFSI sector in India of which One should be a scheduled bank		No Query
143	82	Table 23: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.	Bidder to Comply with RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
144	88	Annexure – 8 Technical Scoring Criteria	Table – 33: Bidders Past Experience Category-1 SIEM Implementation in Organizations b.) The bidder should have successfully implemented proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Request you to kindly consider the projects executed in last five financial years and modify the clause as given below. b.) The bidder should have successfully implemented proposed SIEM solution during any of the last five financial years: 2016-2017, 2017-2018, 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1.
145	88	Table – 33: Bidders Past Experience	b.) The bidder should have successfully implemented proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Requesting KGB to modify the clause as "b.) The bidder should have successfully implemented proposed SIEM solution during any of the last Five financial years:2016-17, 2017-18, 2018-2019, 2019- 2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1.
146	88	Annexure – 8 Technical Scoring Criteria	Table – 33: Bidders Past Experience Only the five references as per Annexure-3 would be considered. The score for this section is the sum of the individual scores of the references provided	We request you to consider 3 projects reference for the purpose of evaluation and providing maximum marks and make the changes to Annexure 8: Table 33(a)/33(b)/33(c) accordingly.	Please refer Amendment No. 1.
147	88	Table – 33: Bidders Past Experience	Category-1 b.) The bidder should have successfully implemented proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Category-1 b.) The bidder should have successfully implemented proposed SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1.
148	88	Annexure-1 Pre-Qualification Criteria	Category 1 b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Request you to kindly consider the projects executedin last five financial years and modify the clause as given below. b.) The bidder should have successfully implemented proposed On-Premise SIEM solution during any of the last five financial years: 2016-2017, 2017-2018, 2018-2019, 2019-2020 and 2020-2021 in any two PSU/PSB/BFSI sector in India, out of which one should be a scheduled bank.	Please refer Amendment No. 1.
149	90	Table – 33: Bidders Past Experience	Category-2 For SI - The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	We request bank to amend the clause as under : For SI - The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI/Govt. sector in India, during any of the last last five financial years: 2016-17, 2017-18, 2018-2019, 2019-2020 and 2020-2021.	Please refer Amendment No. 1.
150	90	Table – 33: Bidders Past Experience	Category-2 For SI - The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	We understand that we can submit saparate PO for each of the technologies, Kindly confirm	Please refer Amendment No. 1.
151	88	89	Table – 33: Bidders Past Experience, Category - 1, Marking for scope of SIEM solution for the references provided Refer Table 33(b) for scoring	Request bank to consider the experience of Bidder/OEM	Bidder to Comply with RFP terms
152	90	Table – 33: Bidders Past Experience Catergory 2	The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021	Requesting KGB to modify the clause as "The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last Five financial years: 2016-17,2017-18,2018-2019, 2019-2020 and 2020-2021	Bidder to Comply with RFP terms
153	90	Annexure – 8 Technical Scoring Criteria	Table – 33: Bidders Past Experience Category-2 For SI - The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last three financial years: 2018-2019, 2019-2020 and 2020-2021.	Request you to kindly consider the projects executed in last five financial years and modify the clause as given below. For SI - The bidder should have successfully implemented: Anti- APT, VM, and PIM in any PSU/PSB/BFSI sector in India, during any of the last five financial years: 2016-2017, 2017-2018, 2018-2019, 2019-2020 and 2020-2021.	Bidder to Comply with RFP terms
154	90	Annexure – 8 Technical Scoring Criteria	Category 2 For VM, Anti-APT and PIM only the five references with the maximum score would be considered. The score for this section is the sum of the individual scores of the references provided.	We request you to consider 3 projects reference for the purpose of evaluation and providing maximum marks and make the changes to Annexure 8: Table 33(a)/33(b)/33(c) accordingly.	Bidder to Comply with RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
155		Additional	Site not ready condition for Implementation payment terms	Request you to include site not ready condition in to payment terms as if due to any challenge from other vendor/site challenge/down time/ other readiness/dependent component for completing implementation.	Bidder to Comply with RFP terms
156	11	4.2 (a)	The C-SOC should be able to identify information security vulnerabilities in Banks environment and prevent these vulnerabilities through implementation of adequate security solutions or controls.	Understanding is that the SI would only monitor the events and incidents. Relevant deployment of solution or technology would be Bank's responsibility.	The deployment of the solutions will be in co-ordination with the Bank and the SI after successful installation the monitoring responsibility of events and incidents will be the responsibility of the bidder
157	12	4.6	Deep Packet Analysis	Please confirm the average bandwidth for the segment which needs to captured via DPI Solution	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
158	12	4.6	Deep Packet Analysis	Please confirm If deep packet inspection with realtime packet analysis & correlation solution is required or only packet capture with forensic capability is required	Packet capture with forensic capability is required
159	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.
160	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 the minimum requirement that has been mentioned. It is up to the bidders to design their solution and have the requirements accordingly.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
161	14	8.5	8.5In case of software-based solution, the bidder needs to propose the minimum level of hardware as below: 8.5.1For SIEM: 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 8.5.2For other solutions (software based), the minimum server sizing expected is: 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 8.5.3For any SIEM device including management servers, the deployment requirement is as per Annexure – 4 Technical Bill of Material. These should be in 1U size if, Physical. 8.5.4The bidders are free to quote blade servers to meet the requirements of this RFP; however, the OEMs for these servers must be in the leader's quadrant for this year's or previous year (2021 or 2020) Gartner Magic Quadrant for Blade servers. 8.5.5The server make proposed should be from reputed manufacturers (data centre class) and should have been deployed by the bidder in other organizations. All servers should meet the below mentioned criteria: a)Server family should have published benchmark SPECint rate and Specify rate benchmark (Supporting documents to be submitted). b)Server family should have published benchmark TPC benchmark. c)Server should have 4*1G integrated on-board ports and should support two embedded 10 Gb Ethernet ports (10GBASE-T RJ-45 or 10GBASE-SR SFP+ based) without consuming PCle slots. d)Should be in the top 5 of IDC's latest worldwide server market review report.	Bidder request to remove this clause due to the following reasons 1. All OEM products does have the required Hardware Sizing specifications as per the System testing, Regression Testing, UAT, integration Testing. So, based on the required workload there is the hardware recommendation which ensures that from capacity prospective same will be fit for purpose. 2. It will be the responsibility of OEM/SI that provided hardware is suitable to cater the workload. 3. There may be some commercial benefits also.	These are the minimum requirements, the bidder is free to propose the optimal solution to the Bank in order the meet the RFP requirements.
162	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	1)Please confirm whether all the components of SIEM need to install on dedicated hardware OR the solution can be virtualized OR appliance based solution. 2)We request bank to allow solution provider to proposed the hardware sizing as per the solution requirement of regardless of minimum sizing requirment as this will resetrict and may end up with High TCO.	1. It is up to the bidder to provide the best optimal solution to the Bank in order to meet the stated RFP requirements. 2. This is only the minimum requirement that has been mentioned. It is up to the bidders to design their solution and have the requirements accordingly.
163	14	8.5.1 (a)	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	Please remove thse clauses and allow the bidder to size the compute configuration basis Application requirements and Sizing for EPS.	These are minimum requirements, it is up to the bidder to size the proposed solution accordingly in order to meet the stated RFP requirements
164	14	8.5.2	8.5.2 For other solutions (software based), the minimum server sizing expected is: 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	As per the rfp clause 8.5.2, the minimum hardware requirement is mentioned for the applications. Each application have their own hardware requirement for the optimal performance, so that we can avoid the over provisioning of hardware. Requesting you to change the cluase as the bidder can choose the hardware resources based on application requirement?, so that we can avoid the over provisioning of hardware.	These are minimum requirements, it is up to the bidder to size the proposed solution accordingly in order to meet the stated RFP requirements
165	14	8.5.4	The bidders are free to quote blade servers to meet the requirements of this RFP; however, the OEMs for these servers must be in the leader's quadrant for this year's or previous year (2021 or 2020) Gartner Magic Quadrant for Blade servers.	Since this is a security SOC Solution Blade/Rack/HCI can be designed basis application ISV and solution requirements. Hence reference to blade may kindly be removed. Also Magic quadrant data available is only till 2017 for traditional servers,	Please refer Amendment No 1

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
166	14	8.5.4	The bidders are free to quote blade servers to meet the requirements of this RFP; however, the OEMs for these servers must be in the leader's quadrant for this year's or previous year (2021 or 2020) Gartner Magic Quadrant for Blade servers.	Since Magic quadrant data available is only till 2017 for traditional servers. Also, this is a security SOC Solution requesting bank to allow bidder to use Blade/Rack/HCI can be designed basis application ISV and solution requirements.	Please refer Amendment No 1
167	15	8.5.5 (a)	a) Server family should have published benchmark SPECint rate and SPECfp rate benchmark (Supporting documents to be submitted).	SpecINT, SpecFB, TPC Benchmarks are not done for every generation of servers. Security solutions requires different paramters to size the hardware as per Application. Hence please remove this clause.	Please refer Amendment No 1
168	15	8.5.5 (b)	b) Server family should have published benchmark TPC benchmark.	SpecINT, SpecFB, TPC Benchmarks are not done for every generation of servers. Security solutions requires different paramters to size the hardware as per Application. Hence please remove this clause.	Please refer Amendment No 1
169	15	8.5.5 (c)	c) Server should have 4*1G integrated on-board ports and should support two embedded 10 Gb Ethernet ports (10GBASE-T RJ-45 or 10GBASE-SR SFP+ based) without consuming PCIe slots. d) Should be in the top 5 of IDC's latest worldwide server market review report.	Onboard integrated controllers have 4 x 1Gb Generally. 10Gb ports have to be added by Mezz card or PCI Cards. Please make two embedded 10Gbs portts as Embedded /LOM /PCI Card based.	Please refer Amendment No 1
170	15	8.5.6 (a)	a) Bidder should not quote hardware which are impending end of sale in 2 yearsfrom the date of submission of bid.	X86 Servers and chipset are fast evolving and new geenration of CPUs, CHIPSETS are released almost every year. HENCE Please change the clause to 1 Year instead of 2 YEAR for end of sale. However support and upgrades will be available .	Bidder to comply with the RFP terms
171	15	8.5.6. (b)	"b)The bidder shall ensure that any additional hardware/software/network equipment required to operationalize the respective solutions/devices must be detailed in the technical and commercial bill of material. If the same is not ensured, the bidder shall be responsible to provide such hardware / software / networking equipment free of cost to the bank at the time of implementation"	Will bank be providing L2 switches for connecting servers? If not, in case of bidder providing L2 switches, what will be the interface available at Bank's DC/DR equipment to which bidder's L2 siwtch can be connected.?	The selected bidder will be provided with the details. In the RFP response the bidder needs to respond to any additional software/hardware needs to be procured by the Bank.
172	15	8.6.1	Develop parsing rules for non-standard logs.	Please share the list of log sources/custom applications for which parser is required.	Please refer to Annexure-7 of the RFP for details
173	16	8.6.3	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
174	16	8.6.3	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
175	16	8.6.3. b)	The bidder shall provide Video Matrix Switch which routes video from computers (Dual Monitors) in C-SOC room to multiple displays (projectors, monitors, etc.). All necessary configuration/implementation of this network is also Bidders Responsibility. The same needs to be covered under the Commercial Bid (CB) / Bill of materials in Technical bid with Models and specifications.	Request to specify the video input & output type(VGA/HDMI) and also the count of input and output. Pls also provide the length of Cables Required. Any civil work required for routing the cables should be done by Bank.	Any civil work will be done by the Bank however as per the requirement in the RFP the bidder needs to provide any additional software/hardware to the Bank and the same to be covered in technical and commercial bill of materials with models and specifications.
176	16	8.6.4	8.6.4 Integration The SIEM tool should be integrated with incident management and ticketing tool to generate automated tickets along with criticality levels for the alert events generated by the SIEM tool. All the security devices/solutions being proposed as part of the current RFP/existing and future devices and solutions identified by the banks need to be included for monitoring by SIEM solution.	pls provide ticketing system tool details and incident management tool	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total SIEM solution
177	16	8.6.4	Security Information & Event Management (SIEM) - 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

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
178	16	8.6.4	The SIEM tool should be integrated with incident management and ticketing tool to generate automated tickets along with criticality levels for alerts events generated by the SIEM tool.	Please share with us the following. 1. Name and version of the Incident management and ticketing tool deployed by Bank. 2. Whether the tool supports API based integration ?	Bank does not poses any incident management tool. Bank expects basic ticketing mechanism has part of the overall SIEM solution
179	16	8.6.4	Security Information & Event Management (SIEM) - Integration	Request bank to provide the details and level of integration require of proposed solution with 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
180	16	8.6.5	The logs collected by SIEM log collector should be replicated across primary Data Centre and DRC.	is this requirement a mandatory requirement or can be treated as a desirable requirement ?	It is a mandatory requirement
181	16	8.6.5	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?	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
182	16	8.6.5	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.
183	16	8.6.5	The logs collected by the SIEM log collector should be replicated across primary Data Center, and Disaster Recovery Centre.	Is the replication only for the Logs or entire system proposed ?	Please refer to Annexure-7. The specified section pertains to the logs only.
184	16	8.6.5	8.6.5 Replication The logs collected by the SIEM log collector should be replicated across primary Data Center, and Disaster Recovery Centre. The bidder needs to provide an estimate of the bandwidth required for the replication process after due analysis of the existing setup at the Bank. Bank shall procure additional bandwidth if required. 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.	Request bank to provide details of existing setup as referred to in the clause for detailed analysis	Will be provided to the selected bidder
185	16	8.6.5	Replication Security Information & Event Management (SIEM) - Replication	Is Replication is in bidder scope? If Yes, please share the detailed requirement.	Replication is with bidder's scope Bidder to comply with the RFP terms
186	16	8.6.6	Storage	Request bank to confirm that the Backup solution be provided by the bank for backing the logs ?	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
187	16	8.6.5	The logs collected by the SIEM log collector should be replicated across primary Data Center, and Disaster Recovery Centre.	Is the replication only for the Logs or entire system proposed ? Please confirm.	Please refer to Annexure-7. The specified section pertains to the logs only.
188	16	8.6.6	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	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
189	17	8.6.6 (c)	The bidder is free to quote either of SAS/SSD for tier 1 storage and SATA/SAS/SSD for tier 2 which meet the requirements	Please allow bidder to chose appropriate stroage solutions for Online and Archival tier and data movement at the overall solution level.	Bidder to comply with the RFP terms
190	17	8.6.6 (d)	The bidder is responsible for automated online replication of logs (online/ archival) from DC to DRC for redundancy.	Is bank using any Backup/Replication tool which can be leveraged for this purpose. Or the bidder has to propose a new tool?	Bidder to comply with the RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
191	17	8.6.6 (e)	The solution should be capable of automatically moving the logs from online to archival storage based on the ageing of the logs. The solution should support object storage to provide protection from attacks such as Ransomware.	Please allow bidder to chose appropriate storgage solutions for Online and Archival tier and data movement at the overall solution level.	The bidder is expected to meet the RFP requirements and to fulfill those requirements the bidder to provide the optimal solution to the Bank
192	17	8.6.6 (f)	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. The solution should have the option to support backup on tape library	Controller based Archival Storage with WORM Capability is available only with few OEMs. Our solution can propose with Read Only Snapshots volumes for Archival Tier and Data Intgegrity or SCALEOUT Server and Software based Archival solutions. Request bank to delete the clause and propose archival solution.	Bidder to comply with the RFP terms
193	17	8.6.6 (f)	f) 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. The solution should have the option to support backup on tape library. g) The storage requirements at a minimum are mentioned below. However, the bidder is expected to size the storage as per the requirements mentioned in the 'Scope of Work' Annexure-7 in this RFP. The bidder's response should include the calculations/ logic used to arrive at the sizing.	The RFP asks for Archival storage that is SAN based, with deduplication and compression. However, in clause f, it does state that the logs should be stored in tamper proof mechanism for online and archival storage. Logs, by nature, are unique and hence, not good candidates for data reduction technologies such as deduplication and compression. Requesting the bank to consider if you are looking for deduplication and compression capability for the Archival storage.	Bidder to comply with the RFP terms
194	17	8.6.6 (g)	Table 1: Minimum Storage Requirements Tier Type Disk RPM RAID Tier-I SAN (SAS / SSD) 15000 (or the latest version available) 5 Tier-II Archival (5 Years), SAN Based with deduplication / compression capability (SATA / SAS / SSD) 7200 (or the latest version available) 5	Please allow RAID 5 /RAID 6 /Erasure coding /2 Copy Data availability options as per solution	RAID 5 has already been mentioned in the RFP requirements
195	17	8.6.6 (i)	i) All storage devices should include at a minimum a dual controller and should be of the following specifications with respect to host connectivity:	The RFP states 8GB FC for host connectivity - the industry standard is ‘Gb - Gigabits’ for denoting FC protocol speed. As per the industry trends, current hosts are offered with 16Gb/32Gb FC ports, as a standard. Requesting the bank to consider at least 16Gb FC ports for host connectivity, to ensure that the bank’s investment in the infrastructure is protected and future proof.	In section 8.6.6 of the RFP 'GB" represents Gigabits. The mentioned specification are the minimum requirements, the bidder is free to propose the optimal solution to the Bank
196	17	8.6.6 (i)	Table 2: Minimum Host Continuity Requirements Host Connectivity 1GB iSCSI 2 Ports/Controller 10GB iSCSI 2 Ports/Controller 8GB FC 4 Ports/Controller Archival storage Connectivity Protocols to be supported: CIFS, NFS & HTTP.	Please allow bidder to chose port count basis the solution sizing and requirements and the topology	These are the minimum set of requirement, the bidder can consider more appropriate solutions in order to meet the requirements of the RFP.
197	18	8.6.7	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: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
198	18	8.6.7	Security Information & Event Management (SIEM) - Packet Capture	For sizing 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 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?	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.
199	18	8.6.7	The Solution must be capable of full packet capture and securely store these packets for a minimum of 30 days.	Please confirm the the number of locations where PCAP solution is required or packet needs to captured	PCAP solutions to be placed both at Bank's DC and DR location

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
200	18	8.6.7	The Solution must be capable of full packet capture and securely store these packets for a minimum of 30 days.	Please confirm the average bandwidth for the segment which needs to captured via Pcap Solution	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
201	18	8.6.7	Security Information & Event Management (SIEM) - Packet Capture	Request bank to share below details for 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.	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: 50 Mbps * Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% * Volume of SSL transactions : 30%
202	18	8.6.8	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
203	18	8.6.8	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
204	18	8.6.8	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

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
205	18	8.6.8	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 server for integration.
206	18	8.6.8	Security Information & Event Management (SIEM) - Incident Management tool	Request bank to confirm on Incident Management Tool asked as a part of SIEM. Can bidder leverage an integrated tool with SIEM or bidder will propose it as a separate ITMS tool.	The bidder should consider it as part of the overall proposed SIEM solution
207	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 / alarm generation systems 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
208	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.
209	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 ?	Please refer Amendment No.1
210	19	8.9.1 (b)	Configure the vulnerability management policies and manage the vulnerabilities across vulnerability management life cycle.	Understanding is that we need to coordinate with the device management team of bank to close vulnerability or execute remedial action. Remediation will not be our resposibility, except for devices supplied and managed under the scope of work.	It is expected that SI to co-ordinate with the respective team to close the reported vulnerabilities and suggest the remediation methods for the reported vulnerabilities to the Bank in co-ordiantion with the Bank information security team.
211	21	9.2 (d)	In addition, the bidder is responsible for impact assessment and modification of C-SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations.	We request Bank to modify this clause as this is an open ended statement. An impact of a change of security policy by either the Bank or any regulatory compliance might require additional technology solution, which comes at additional cost and cannot be offered free of cost.	Bidder to comply with RFP terms
212	21	9.2 (f)	j)Post initial implementation, the bidder is responsible for integrating any additional logs that the bank may wish to monitor with the SIEM solution at no additional cost to the banks.	Bidder request to share the probable count of devices or device types, log types for which the additional logs collection may be required in future. It will help us to understand the effort estimation and cost accordingly	Bidder to comply with the RFP terms
213	21	9.2 (g)	Any interfaces required with existing applications/ infrastructure within the bank should be developed by the bidder for successful implementation of the C-SOC as per the defined scope of work.	Bank needs to provide the list of applications intended to be integrated wit the SIEM solution. This will help us assess the number of custom interface development required.	Please refer to Annexure-7 for details
214	22	9.7	The bidder is responsible for defining a DRC/BCP plan for the SOC operations and ensure that periodic tests are conducted as per the testing requirements of the Banks.	Please share the RTO / RPO for the DR.	Bank will work with the selected bidder in order to determine the RTO/RPO for the SOC operations

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
215	22	9.7	The bidder is responsible for defining a DRC/BCP plan for the SOC operations and ensure that periodic tests are conducted as per the testing requirements of the Banks.	Do we need to consider the Manual DR or Automated with DRM Tool?	The selected bidder needs to work with the bank for formulation of DRC/BCP plan for the SOC operations and suggest the bank optimal methods for disaster recovery
216	22	9.7	The bidder is responsible for defining a DRC/BCP plan for the SOC operations and ensure that periodic tests are conducted as per the testing requirements of the Banks.	Requesting you to share the DR expectation with more details.	The selected bidder needs to work with the bank for formulation of DRC/BCP plan for the SOC operations and suggest the bank optimal methods for disaster recovery
217	22	9.7	The bidder is responsible for defining a DRC/BCP plan for the SOC operations and ensure that periodic tests are conducted as per the testing requirements of the Banks.	Please share the RTO / RPO for the DR. Also, is banking looking for Manual or Automated DRM.	Bank will work with the selected bidder in order to determine the RTO/RPO for the SOC operations
218	29	23.3	All the in-scope solutions should be implemented parallelly. PIM - T+18 Weeks Anti-APT - T+12 Weeks VM - T+8 Weeks	Considering Covid-19 Pandamic, requesting bank to relax the stringint timeline.	Please refer Amendment No 1
219	33	25.2 Table 7	SLA - 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 event identification. High Priority - within 30 minutes of event identification. Medium - within 60 minutes of event identification.	Giving a mitigation step of action plan for critical events is not possible in 15 minutes, hence we request bank to amend these SLA as follows **Time to Notify (this is the time to notify about an incident)** **Critical - 15 minutes** **High - 30 minutes** **Medium - 60 minutes** **Time to Triage (this is the time taken by Analyst to perform and conduct first responder processes)** Critical - 60 minutes High - 90 minutes Medium - 120 minutes **Time to Diagnose(this is the time taken by Analyst to perform detailed analysis and provide recommendation and response steps** Critical - 120 minutes High - 180 minutes Medium - 240 minutes	Bidder to comply with the RFP terms
220	33	25.2 Table 7	Incident Resolution	Incident Resolution for any other devices/services,except for components supplied by SI is not in SI scope. This would be the responsibility of Bank's managed service provider or team managing those devices	Bidder to comply with RFP terms
221	33	25.2 - Table – 7	DailyReports:Criticalreports should be submitted twice a day. (First report at 10 am and second report at 5pm every day). •Delay in reporting for daily report for more than 2 hours shall incur a penalty of 3% of Monthly CSOC Resource Cost Weekly Reports: By 10:00 AM, Monday MonthlyReports:5th of each calendar month •Delay in reporting by more than 1 day for weekly and 3 days for monthly reports shall incur a penalty of 10% of Monthly CSOC Resource Cost	Bidder request to remove the Daily report delay penalty as there is already a penalty on Weekly and Monthly reports. Also, Bidder request to keep the daily report at 10 AM daily as per the industry standards and best practices.	Bidder to comply with the RFP terms
222	60	56	Support for maintenance of Hardware, software (including OS and software license) and Other Items supplied should be available for a minimum period of 3 years, covering all parts, maintenance, and support, after expiry of warrantyperiod	We offer our services from a Shared Cloud Platform which is hosted in a MeitY approved DC in India. Only the sensors such as scanner and agents need to be deployed in the bank's premises. Hence, we request the bank to accept the subscription to our shared cloud platform	Bidder to comply with RFP terms.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
223	61	57.5	The selected bidder shall grant an irrevocable perpetual license to the Bank to use the software. Further, all software supplied shall be of latest version.	We request the bank to consider annual subscription based licensing model	Bidder to comply with the RFP terms
224	1 of 25	Annexure-2, SIEM - point 2	2. The proposed solution licensing should be by the number of events per second	Please change it to Licensing should be based on the number of devices and EPS	Bidder to comply with RFP terms - Please refer Annexure -7 for details of devices to be integrated
225	1 of 25	Annexure-2, SIEM - point 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
226	2 of 25	Annexure 2, SIEM - point 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 custom connectors could be built by bidder / provider. Request Bank to modify as appropriate.	Bidder to comply with the RFP terms
227	2 of 25	Annexure -2, SIEM - point 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	Please share the list of devices/applications.	Please refer to Annxeure-7 for the list of devices to be integrated with the SIEM solution
228	2 of 25	Annexure -2, SIEM - point 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.	Bidder to comply with the RFP terms
229	3 of 25	Annexure -2 , SIEM - point 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 (g) table-1 of the RFP for more details.
230	3 of 25	Annexure -2 , SIEM - point 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	Raw logs for analysis purpose
231	3 of 25	Annexure -2 , SIEM - point 28	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	The proposed solution should support the following log collection protocols: Syslog over UDP / TCP, Syslog NG, SDEE, SNMP Version 2 & 3, ODBC/JDBC, FTP, Windows Event Logging Protocol, Opsec, Netflow at a minimum.	Bidder to comply with RFP terms
232	3 of 25	Annexure -2, SIEM - point 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 the RFP terms
233	4 of 25	Annexure 2, SIEM - point 32	Sl.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?	The Threat intelligence feeds has to be bundled as part of the proposed solution
234	6 of 25	Annexure- 2, SIEM - point 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
235	6 of 25	Annexure- 2, SIEM - point 55	The proposed solution should provide knowledge base and best practices for various security vulnerabilities	This funtionality is related to vulnerability management solution, hence request to please move this point to the VM section.	Bidder to comply with the RFP terms
236	7 of 25	Annexure -2, SIEM - point 58	58. Dashboard should support monitoring, alerting and reporting for consolidated relevant compliance across all major standards and regulatory requirements in real time. This includes (but not limited to): ISO 27001, RBI regulations, IT ACT, PCI DSS standards, and NABARD regulations	Dashboard should support monitoring, alerting and reporting for consolidated relevant compliance across all major standards and regulatory requirements in real time. This includes (but not limited to): ISO 27001, RBI regulations, IT ACT, PCI DSS standards, and NABARD regulations using natively or customized Dashboard	Bidder to comply with RFP terms
237	7 of 25	Annexure -2, SIEM - point 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 the RFP terms
238	7 of 25	Annexure -2, SIEM - point 63	Senior Management should be able to view compliance to SLA for all SOC operations	This functionality is related to Incident management tool, hence request to please move this point to Incident management section.	Bidder to comply with the RFP terms
239	7 of 25	Annexure -2, SIEM - point 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

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
240	7 of 25	Annexure 2, SIEM - point 68	The proposed solution should be possible to automatically create incidents and track their closure	Kindly clarify whether the incident management tool to be proposed as a seperate tool or can it be an integrated component of the SIEM solution	The incident management tool should be a part of the overall proposed SIEM solution
241	7 of 25	Annexure 2, SIEM - point 68	Sl.No. 68 The proposed solution should be possible to automatically create incidents and track their closure	Does the bank already have any incident management tool which can be leveraged? Kindly mention the tool name if any.	Bank do not have any incident management tool
242	8 of 25	Annexure -2, SIEM - Point 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 parseris 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
243	8 of 25	Annexure 2, SIEM - point 70	Sl.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
244	8 of 25	Annexure -2, SIEM - Point 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
245	8 of 25	Annexure -2, SIEM - Point 70	Pre-defined parsers are available for parsing logs for Bank's Core Banking Solution (Finacle v7.0.18)	Request to amend as "Proposed solution 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
246	8 of 25	Annexure -2 , SIEM - point 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
247	8 of 25	Annexure -2 , SIEM - point 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 parseris 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
248	8 of 25	Annexure -2, SIEM - Point 71	The proposed solution should be able to conduct full packet capture and securely store these packets for a minimum of 30 days	Not a standard SIEM requirement Recommended integartion with PCAP tool need details on deployed PCAP tool	Currently no PCAP tool is available. Bidder is expected to conduct full packet capture.
249	8 of 25	Annexure 2, SIEM - point 71	Sl.No. 71 The proposed solution should be able to conduct full packet capture and securely store these packets for a minimum of 30 days	What is the sizing requirement for full packet capture in Mbps or Gbps?	With the internet bandwidth throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. LAN bandwidth : 1 Gig / 10Gig. 4. Channel : DC & DR : Copper and Fibre.
250	8 of 25	Annexure -2, SIEM - Point 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

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
251	8 of 25	Annexure -2 , SIEM - point 71	The proposed solution should be able to conduct full packet capture and securely store these packets for a minimum of 30 days	What is the sizing requirement for full packet capture in Mbps or Gbps?	With the internet bandwidth throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. LAN bandwidth : 1 Gig / 10Gig. 4. Channel : DC & DR : Copper and Fibre.
252	8 of 25	Annexure -2 , SIEM - point 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
253	8 of 25	Annexure -2 , SIEM - point 73	The proposed solution must provide embedded workflow capabilities that security operations staff can use to guide their work	This functionality is related to Incident management tool, hence request to please move this point to Incident management section.	Bidder to comply with the RFP terms
254	8 of 25	Annexure -2 , SIEM - point 75	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.	This functionality is related to Incident management tool, hence request to please move this point to Incident management section.	Bidder to comply with the RFP terms
255	8 of 25	Annexure -2, SIEM - Point 77	The proposed solution should be able to perform full reconstruction of session / events.	Recommendation: Not a standard SIEM requirement The above funtionality can be achieved by integration with any third party PCAP tool Ammendment: Solution should be able to integrate with 3rd party PCAP tool to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.	Bidder to comply with the RFP terms
256	8 of 25	Annexure -2, SIEM - Point 78	Support importing of PCAP files, other structured and unstructured content for analysis.	For sizging the packet capture, please rpbvide the belo 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?	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.
257	9 of 25	Annexure 2, SIEM - point 84	Sl.No. 84 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	Kindly help define Tier I and Tier II storage in terms of type of storage devices and mechanisms.	Please refer to section 8.6.6 (g) table-1 of the RFP for more details.
258	9 of 25	Annexure -2, SIEM - Point 84	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
259	9 of 25	Annexure -2, SIEM - Point 84	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	Kindly confirm does Bank provides the storage or Bidder should consider the stroge for SIEM Solution.	The bidder should provide the storage for SIEM solution
260	10 of 25	Annexure 2, SIEM - point 97	Sl.No. 97 The proposed solution should be able to Integrate with helpdesk/ ticketing tools	Does the bank have a ticketing system in place and which solution. Incase not available, is the Bank expecting the bidders to provision the same?	Bank expects a basic ticketing functionality as part of a overall proposed SIEM solution in order to assign incidents to the respective team member

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
261	10 of 25	Annexure -2, SIEM -point 97	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 Bank is currently using CA tool.
262	10 of 25	Annexure -2, SIEM -point 98	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.	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
263	10 of 25	Annexure 2, SIEM - point 98	Sl.No. 98 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?	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
264	10 of 25	Annexure -2, SIEM -point 98	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.	The proposed solution should be able to integrate with the Bank's existing VEEAM backup solution
265	10 of 25	Annexure 2, SIEM - point 101	Sl.No. 101 Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications	Can you define the number of such home-grown/unsupported applications	Please refer Table-27 for the listed devices the bidder has to develop security related use cases in conjunction with the bank.
266	10 of 25	Annexure 2, SIEM - point 103	Sl.No. 103 The proposed system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.	Please share the list of IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, databases and standard applications.	Please refer Annexure - 7 table no 26,27 and 28 for details
267	10 of 25	Annexure 2, SIEM - point 105	Sl.No. 105 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 the RFP terms
268	10 of 25	Annexure -2 , SIEM - point 105	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 the RFP terms
269	10 of 25	Annexure -2 , SIEM - point 105	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 the RFP terms
270	11 of 25	Annexure 2, SIEM - point 107	Sl.No. 107 The proposed solution should be scalable as per bank roadmap for expansion	What would be a tentative scalable roadmap for expansion in the coming years, in terms of EPSsizing and Packet Capture sizing for the next few years?	Please refer to Annexure-7 for details and the bidder has to analyze the packet capture size.
271	11 of 25	Annexure -2 SIEM - Point 107	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 and the bidder has to analyze the packet capture size.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
272	11 of 25	Annexure -2 SIEM - Point 111	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 are 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 111 is preferable in nature.
273	11 of 25	Annexure -2 SIEM - Point 111	The proposed solution should be preferably appliance-based solution	Next Gen SIEM tools are generally offered as a Software based solution on dedicated hardware which supports horizontal scalability as per requirement in future	Please refer point-1 of Annexure-2 Technical Requirements
274	11 of 25	Annexure 2, SIEM - point 111	Sl.No. 111 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 111 is preferable in nature.
275	11 of 25	Annexure -2, SIEM - point 111	The proposed solution should be preferably appliance-based solution	This clause conflicts 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 111 is preferable in nature.
276	11 of 25	Annexure -2, SIEM - point 111	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 are to be considered or software with servers or any of them can be proposed? 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 111 is preferable in nature.
277	11 of 25	Annexure -2 SIEM - Point 112	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.
278	11 of 25	Annexure 2, SIEM - point 112	Sl.No. 112 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.
279	12 of 25	Annexure -2, PIM - point 2	The proposed solution should provide the feature of keystroke logging for privileged users	Pls help us understanding this requirement better.	For all the privileged users the solution should be able to capture all the action of recording the keys struck on a keyboard.
280	12 of 25	Annexure 2, PIM - point 8	The proposed solution support delegation by identity administrator to another person for a specific period of time	Is this requirement revolves around PIM administration delegation for a defined period?	Time-specific administrator access can be provided to a specific user
281	12 of 25	Annexure -2, PIM - point 9	The proposed solution support for reminders to identity administrators who are required to perform workflow tasks	Is this requirement revolves around PIM administration for requests access approval workflows?	Bidder to comply with RFP terms
282	13 of 25	Annexure -2, PIM - point 12	The proposed solution should enforce segregation of duties as defined by the Bank.	Can you please help in understanding the use-case of segregation of duties.	Role base access to be provided

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
283	13 of 25	Annexure 2, PIM - point 16	S.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	The bidder shall propose the solution which is capable to develop compliance reports in order to meet Bank's regulatory requirements.
284	13 of 25	Anenxure -2, PIM - point 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.	Specific compliance reporting is generally feature of Audit reporting tools and is not the core function of PIM. We suggest to modify it as below: "Proposed PIM should help in complying with PCI DSS, RBI Guidelines, NABARD regulations, Cert-In, NCIIPC and others."	The proposed solution should provide PIM audit reports in order to meet Bank regulatory requirements. Bidder to comply with the RFP terms
285	13 of 25	Annexure -2, PIM - point 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.	Specific compliance reporting is generally feature of Audit reporting tools and is not the core function of PIM. We suggest to modify it as below: "Proposed PIM should help in complying with PCI DSS, RBI Guidelines, NABARD regulations, Cert-In, NCIIPC and others."	The proposed solution should provide PIM audit reports in order to meet Bank regulatory requirements. Bidder to comply with the RFP terms
286	13 of 25	Annexure 2, PIM - point 17	The proposed solution should include a software development kit to facilitate integration with home-grown/ in-house applications	CyberArk Privileged Access Security solution have exposed APIs for integration with applications. Pls help us understand the integrarion requirement here. Is there any requirement for managing application connection strings in CyberArk? If yes, pls share application technology details.	Access approval and request workflows and others are required to be designed in PIM solution
287	13 of 25	Annexure -2, PIM - point 17	The proposed solution should include a software development kit to facilitate integration with home-grown/ in-house applications	Can you please share details of home-grown applications to be integrated. How these applications being accessed, using web access or thick-client based access, or any other method?	Please refer to Table-28 under Annexure-7 of the RFP for more details. The selected bidder will be provided with the details
288	13 of 25	Annexure -2, PIM - point 18	The proposed solution should be able to integrate with existing AAA authentication devices, directory services etc.	Can you please share deails of existing AAA solution.	The details will be shared with the selected bidder.
289	13 of 25	Annexure -2, PIM - point 18	The proposed solution should be able to integrate with existing AAA authentication devices, directory services etc.	Can you please share details of existing AAA solution.	The details will be shared with the selected bidder.
290	13 of 25	Annexure -2 , PIM - point 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.	Any changes in the event logs should be monitored and maintained
291	13 of 25	Annexure -2, PIM - point 20	The proposed solution should have template-based workflows for user account creation, management, group assignments, de-activation and deletion	Is there any Identity and Access Management tool already in place? If yes, please share make & model	Bidder to comply with the RFP terms
292	13 of 25	Annexure -2, PIM - point 22	The proposed solution should support both workflow for disabling and deletion of accounts in separate steps as per Bank's requirements.	Workflows are generally function of IDAM solution. Is there any existing IDAM solution already in place or bidder should propose as part of solution?	The bidder should propose the PIM/PAM solutions to the Bank in order to meet the Bank's requirement
293	13 of 25	Annexure -2, PIM - point 23	The proposed System should have a web-based GUI for designing workflows	Pls elaborate on what kind of workflows are required to be designed in PIM solution?	Access approval and request workflows are required to be designed in PIM solution
294	14 of 25	Annexure -2, PIM - point 26	The proposed system should support integration with external GRC, SIEM and HRMS	Pls let us know which external GRC, SIEM and HRMS is in use. Also, pls help us understand the kind of integration required for all uf such external tools.	Currently there is no GRC tool implemented within the Bank environment. The proposed SIEM solution should be able to integrate with the third party GRC solutions. Currently bank is using SAP based HRMS.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
295	14 of 25	Annexure -2, PIM - point 26	The proposed system should support integration with external GRC, SIEM and HRMS	Is there any existing GCRC solution in place? Please elaborate the use-case for integration with HRMS.	Currently there is no GRC tool implemented within the Bank environment. The proposed SIEM solution should be able to integrate with the third party GRC solutions. Currently bank is using SAP based HRMS.
296	14 of 25	Annexure 2, PIM - point 28	S.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	This requirement is preferable in nature and not an essential requirement.
297	15 of 25	Annexure -2, PIM - point 43	The proposed solution should be able to integrate with vulnerability management solution to ensure that automated VA scans utilize privileged accounts for devices which are managed by the PIM solution	Pls let us know which VA solution is being used.	The proposed SIEM solution should be able to integrate with the VM solution which the bidder proposes as part of the RFP requirement
298	16 of 25	Annexure -2, PIM - point 50	The proposed solution should provide notifications when privileged roles are activated	Pls help us understanding this requirement better.	Notification on privileged role/access provisioning to a specific user
299	17 of 25	Annexure -2 , Anti-APT - point 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 proposed solution is able to scan more file types, the bidder is welcome to propose the respective solution
300	17 of 25	Annexure -2 , Anti-APT - point 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 is welcome to propose the respective solution
301	17 of 25	Annexure -2 , Anti-APT - point 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
302	17 of 25	Annexure 2, Anti-APT - point 7	Sl.No. 7 The solution should be able to detect and prevent bot outbreaks (via multiple channels like SMTP, HTTP, HTTPS etc.) including identification of infected machines	This largely focus on email traffic and hence Email Anti-APT appliance is required to monitor SMTP traffic.	Please refer Amendment No 1
303	17 of 25	Annexure -2 , Anti-APT - point 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?	Bidder to meet the mentioned requirements and propose the solution accordingly
304	18 of 25	Annexure -2, Anti-APT - point 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 to provide additional features apart from the mentioned requirements within the RFP.
305	18 of 25	Annexure -2, Anti-APT - point 9	The solution should be able to block the call back tunnel including fast flux connections.	Additonally, 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 to provide additional features apart from the mentioned requirements within the RFP.
306	18 of 25	Annexure -2, Anti-APT - point 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 solution to be integrated with the proposed SIEM solution. The details of OEM will be shared with the selected bidder.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
307	18 of 25	Annexure 2, Anti-APT - point 13	Sl.No. 13 The solution should be able to conduct forensic analysis on historical data.	This a use case of an SIEM solution. No Historical analysis, but appliances Supports the retroactive detection feature, it allows the Network Security appliance to alert on missed objects when a hash match happens during an unlimited time period against non-malicious submissions. This feature uses object hashes to alert on missed detections.	A preferrable feature to have in the recommended Anti-APT solution to integrate with the SIEM solution.
308	18 of 25	Annexure -2, Ant - APT - point 13	The solution should be able to conduct forensic analysis on historical data.	This a use case of an SIEM solution. No Historical analysis, but appliances Supports the retroactive detection feature, it allows the Network Security appliance to alert on missed objects when a hash match happens during an unlimited time period against non-malicious submissions. This feature uses object hashes to alert on missed detections.	A preferrable feature to have in the recommended Anti-APT solution to integrate with the SIEM solution.
309	18 of 25	Annexure 2, Anti-APT - point 19	Sl.No. 19 The solution should display the geo-location of the remote command and control server.	We specifically highlight APT alerts and APT's typically nation/state sponsored attacks. Hence this point doesn't bring relevance for an Anti-APT technology.	As, it is a preferrable feature to have geo-lookups for the IPs, from the proposed Anti - APTsolution.
310	18 of 25	Annexure 2, Anti-APT - point 20	Sl.No. 20 The solution should be able to integrate with the Active Directory / ICAP to enforce user-based policies.	ICAP integration can be done. In APT framework there is no use case of use based policies as APT alerts are treated as most critical alerts hence the policy will be applied globally, IP based exception can be made.	Please refer Amendment No 1
311	19 of 25	Annexure 2, VM - point 1	S.No. 1 The proposed solution should have minimal impact on traffic, server performance, networks etc. during deployment and operation	What is the minimial impact ratio or parameter . Please clarify?	Minimal impact means, while running VM scan in the production environment there should not be any significant impact during the business hours in functioning of the applications.
312	19 of 25	Annexure -2 , VM - point 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 during the business hours in functioning of the applications.
313	19 of 25	Annexure -2 , VM - point 3	The proposed solution should provide flexible deployment of VAS solution and capability for tuning the scanning configurations for optimal performance of Bank's infrastructure	Please mention the integration of security solutions which Bank needs	Please refer to section-8 and Annexure-7 of the RFP for more details
314	19 of 25	Annexure 2, VM - point 4	S.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 for more details
315	19 of 25	Annexure -2 , VM - point 5	The proposed solution should perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).	Application scanning please clarfiy internal or external?	Bank will utilize the VM tool for scanning both external and internal facing applications.
316	19 of 25	Annexure 2, VM - point 6	S.No. 6. The proposed solution should support application scanning, endpoints (laptops or desktops) scanning	Application scanning please clarify internal or external?	Bank will utilize the VM tool for scanning both external and internal facing applications.
317	19 of 25	Annexure -2 , VM - point 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.
318	19 of 25	Annexure 2, VM - point 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.	It is a preferrable feature for the recommended solution. Bidder to comply with the RFP terms
319	20 of 25	Annexure 2, VM - point 16	The proposed solution should be able to run scans on network segments as well as entire network.	Please share the database lists as to ensure compatability.	Bidder to comply with the RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
320	20 of 25	Annexure 2, VM - point 18	S.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
321	21 of 25	Annexure 2, VM - point 28	The proposed solution should include a library of potential vulnerabilities and rules which should cover SANS top 20. This library should be customizable by the administrator and changes to the same should be traceable.	This is can be achieved integrating ITSM solution.Request you to kindly let us know what ITSM solution Bank is using	Bidder to comply with the RFP terms
322	21 of 25	Annexure 2, VM - point 30	The proposed solution vendor should assist the bank in reducing the number of false positives identified by the solution	Please share the vendor names of the solutions mentioned to integrate	Bidder to comply with the RFP terms
323	21 of 25	Annexure 2, VM - point 32	S.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 to comply with the RFP terms
324	21 of 25	Annexure -2 , VM - point 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 to comply with the RFP terms
325	21 of 25	Annexure -2 , VM - point 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.	Pleae share the use case for the integration on WAF and mention the vendor name for WAF	Bidder to comply with the RFP terms
326	21 of 25	Annexure 2, VM - point 34	S.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 RFP terms.
327	21 of 25	Annexure 2, VM - point 36	S.No. 36 The proposed solution should integrate with the existing/ proposed WAF solution	Please share the use case for the integration on WAF and mention the vendor name for WAF	It is preferrable feature. Bank will share WAF details with the selected bidder.
328	21 of 25	Annexure -2 , VM - point 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	It is preferrable feature. Bank will share WAF details with the selected bidder.
329	21 of 25	Annexure 2, VM - point 37	S.No. 37 The proposed solution should support integration with threat feeds, allowing vulnerabilities to be correlated against real-time threat information.	Please share the use case for the integration on TI platform and mention the vendor name for WAF	The bidder shall help the Bank in developing use cases for the integration of TI platform , add new use cases for SOC maturity and fine tune the use cases on a periodic basis.
330	21 of 25	Annexure -2 , VM - point 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	The bidder shall help the Bank in developing use cases for the integration of TI platform , add new use cases for SOC maturity and fine tune the use cases on a periodic basis.
331	21 of 25	Annexure -2 , VM - point 42	The proposed solution should support scanning of virtualization and terminal platforms like vSphere, Hyper-V, XenApp, etc.	Please share the vendor for asset managenent tool and the use case	It is a preferable feature. There is no asset management system available with the Bank.
332	22 of 25	Annexure 2, VM - point 47	S.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	It is a preferable feature. There is no asset management system available with the Bank
333	23 of 25	Annexure 2 Other General Requirements - point 2	Sl.No. 2 All solutions should support 256 bit or higher encryption for transfer of information	Need more information's on this requirement.?	The logs and data from all solutions should support 256 bit or higher encryption when shared over Banks network for transfer of information.
334	23 of 25	Annexure 2 Other General Requirements - point 2	Sl.No. 2 All solutions should support 256 bit or higher encryption for transfer of information	The best practise is to have SIEM integration.	The logs and data from all solutions should support 256 bit or higher encryption when shared over Banks network for transfer of information.
335	23 of 25	Annexure - 2, Other General requirements - 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 data bases.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
336	23 of 25	Annexure - 2, Other General requirements - 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.	Understanding is correct.
337	23 of 25	Annexure -2, Other General Requirements - point 12	All the proposed solutions should support external storage such as SAN storage	The best practise is to have SIEM integration.	It is up to the bidder to provide the best optimal solution to the Bank in order to meet the stated RFP requirements.
338	24 of 25	Annexure-2, other General requiremenrts - point 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 understanding is correct.	Bidder to provide threat feeds from the mentioned resources and integrate with the SIEM
339	24 of 25	Annexure 2 .Other General Requirements - point 25	Sl.No. 25 All solutions should be saleable as per Banks future requirements.	The RFP does not mention the future requirements, kindly clarify what is the furture scalability required by the Bank.	Please refer Amendment No 1
340	1 of 4	Annexure 4 (SIEM)	SSL Decrypter	Need details on the number of transaction/connections per second required and also the number of interfaces. Also, if bank had details pertaining to the encryption key size and the Ciphers used on their applications	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. Volume of SSL transactions : 30% 4. Bank is currently using standard Ciphers which supports TLS 1.2 and above.
341	1 of 4	Annexure 4 (SIEM)	SSL Decrypter	Can the bidder propose a single SSL decrypter solution for the multiple products asked in the RFP.	The bidder to provide an optimal solution to meet the stated RFP requirements
342	1 of 4	Annexure 4 (SIEM)	SSL Decrypter	For SSL Decrypter, Request bank to share the inputs on below inputs: 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: 50 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.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
343	1 of 4	Annexure 4 (SIEM)	Annexure-4-Technical-Bill-of-Material	In Annexure 4 - Technical Bill of Material, against the SIEM module, Bank has asked for product and hardware details of SSL Decrypter (HA in DC and standalone in DR). We do not see any specifications for an SSL Decrypter anywhere in the RFP document. Please provide details like the maximum planned throughput for each location, the no. of SSL connections per second, whether traffic is HTTPS alone, the ciphers used by the Bank (RSS or ECC).	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. Volume of SSL transactions : 30% 4. Bank is currently using standard Ciphers which supports TLS 1.2 and above.
344	1 of 4	Annexure 4 (SIEM)	Annexure-4-Technical-Bill-of-Material	In Annexure 4 - Technical Bill of Material, against the SIEM module, Bank has asked for product and hardware details of SSL Decrypter (HA in DC and standalone in DR). We do not see any specifications for an SSL Decrypter anywhere in the RFP document. Please provide details like the maximum planned throughput for each location, the no. of SSL connections per second, whether traffic is HTTPS alone, the ciphers used by the Bank (RSS or ECC).	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. Volume of SSL transactions : 30% 4. Bank is currently using standard Ciphers which supports TLS 1.2 and above.
345	1 of 4	Annexure 4 SIEM	Annexure-4-Technical-Bill-of-Material	we do not see any specifi cati ons for the same in the RFP. We wouldappreciate if Bank can come out with those specifi cati ons like maximum throughput, volume of SSL transacti ons, ciphers used by Bank etc. This would help thebidders to size the appliances keeping in mind the fact that going forward all cyber traffi c would be encrypted	With the internet throughput of the Bank and as per Annexure-7 requirements, the Bidder needs to analyze and propose the solution accordingly. 1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. Volume of SSL transactions : 30% 4. Bank is currently using standard Ciphers which supports TLS 1.2 and above.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
346	1 of 4	Annexure 4 SIEM	Annexure-4-Technical-Bill-of-Material	We would also like to menti on here that while traditi onal security devices can inspect HTTP traffi c, they cannot inspect SSL or encrypted traffi c without incurringheavy CPU resources (up to 60%). This limited functi onality of traditi onal security devices is a concern as the volume of encrypted traffi c is increasing and is expectedto surpass the volume of unencrypted traffi c. Considering the immense possibility of cyber threats propagati ng through encrypted traffi c, it is essenti al thatorganizati ons confi gure their security devices to inspect both encrypted and unencrypted traffi c. In this context, we would recommend to deploy a dedicated SSL Insight (SSLi) appliance in the Bank as part of the C-SOC to decrypt SSL traffi c, which can then beanalyzed by any and all security devices in your environment. Since the encrypti on and decrypti on functi ons are performed by the SSLi device, there is minimumlatency in the network. This would also reduce sizing for the other security devices like SIEM, Anti -APT etc. considerably as the enti re SSL decrypti on/encrypti on isdone in a separate appliance. This would ensure that the overall ROI for your C-SOC would be the same if not much better.	Bidder to comply with RFP terms
347	1 of 4	Annexure 4 SIEM	Annexure-4-Technical-Bill-of-Material	As standard and best practice PCAP & DPI solution are deployed in standalone mode, otherwise Hardware & Storage requirements increases, hence we request to please remove HA from PCAP & DPI solution.	Bidder to comply with the RFP terms
348	2 of 4	Annexure 4 (SIEM)	Security Information and Event Management (SIEM):10,000 - 30,000 (EPS)	Pl clarify if we need to factor 30000 EPS from day 1. The same has a great impact on commercials. Can we request the data log ingestion per day Realistic Projection - The sizing is based on the number of devices that need to considered for log ingestion (GB logs per day). Alternately, the current figure of EPS can be ascertained from the current MSP and then factoring the growth of logs per year, leading to the figure of optimized EPS count.	The initial licensing for EPS is of 10,000. With the rise in EPS count Bank may procure additional licenses.
349	4 of 4	Annexure 4 VM	As per the dvice count and Server Count Bank has total of 759 Devices and servers. And opting for 100 Ips for VM.	Request Bank to Increase the IP count to 512 as per the device and server count for VM.	Bank may increase the IP count for VM in future, bidder to quote for additional IPs in commercial bill of material
350	84	Annexure 7 - 3 (c)	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.	Please refer to section 24.3 (b) and Annexure-6 for more details.
351	85	Annexure 7 - Table 27	Table 27: Other devices to be monitored Table 27: Applications to be Monitored	1. Table 27 shows the different OS platform, does the bank wants to analyse the logs of these OS platform or the applications running on these platform 2. What are these applications and are there any custom built applications? 3. Can the bank share more details on the custom applications if any	Please refer Table-27 for the listed devices the bidder has to develop security related use cases in consultation with the bank. For further details please refer to RFP requirements. Point no 2 and 3 will be provided to selected bidder.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
352	86	Annexure 7 - Table 28	The vulnerability management tool would require to be deployed Primary Data Center for the following number of IPs. The bidders should also quote the additional cost in buckets of 50 IPs.	1)the total no of licenses asked for VA is 100. Considering the size we request the bank to please cosndier VA from a Shared Cloud Platform which is hosted in a MeitY approved DC in India. Only the sensors such as scanner and agents need to be deployed in the bank's premises. Hence, we request the bank to accept the subscription to our shared cloud platform 2)As per the scope of Network(109) and other devices(650) mentioned in the DC & DR, it seems that the vulnerability management scope in the environment would be more than 100 Ips. We request the bank to confirm the exact scope for VM.	Bidder to comply with the RFP terms
353	86	Annexure 7 - Table 28	1 CBS (Finacle) 2 Internet Banking Solution 3 Mobile Banking Solution 4 SFMS (NEFT/RTGS) 5 Unified Payment Interface (UPI) 6 Financial Inclusion Applications	There are internet,mobile,CBS applications mentioned in the list as part of scope. Kindly elaborate on the web applications scope and the number.	All the mentioned applications have web layer
354	Additional Point to be included	NA	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.	1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40% 3. Volume of SSL transactions : 30%
355	Additional Point to be included	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.
356	Additional Point to be included	NA	Additional clarification for Anti-APT	Application control database must contain more than 6000 known applications.	Bidder to comply with RFP terms.
357	Additional Point to be included	NA	Additional clarification for Anti-APT	The solution should have mechanisms to protect against spear phishing attacks	Bidder to comply with RFP terms.
358	Additional Point to be included	NA	Additional Point	Kindly clarify the number of segments to be monitored for Anti-APT and Packet capture solutions as defined in the RFP.	Bidder to comply with RFP terms.
359	Additional Point to be included	NA	Additional Point - Suggestions for amendments Anti-APT	Proposed solution should be independent of existing Firewall, IPS, Proxy etc. so that in future if bank decide to replace any of these components solution should be able to work independently without a need of additional investment.	Bidder to comply with RFP terms.
360	Additional Point to be included	NA	Additional Point - Suggestions for amendments Anti-APT	The solution should support concurrent execution of (but not limited to) " virtual machines so as to enable parallel analysis of multiple objects coming in the web traffic stream without impacting performance	Bidder to comply with RFP terms.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
361	Additional Point to be included	NA	Additional Point - Suggestions for amendments Anti-APT	Proposed Web APT solution should also have SSL Intercept capability (100% SSL traffic performance) to examine encrypted user bound traffic to detect threats (such as CnC traffic and data exfiltration) that attackers may hide in encrypted streams. If solution does not have native SSL capability, 3rd party SSL solution must be factored.	Bidder to comply with RFP terms.
362	Additional Point to be included	NA	Additional Point - Suggestions for amendments Anti-APT	The proposed solution should have the ability to be deployed in the following modes: - inline blocking - inline monitoring and, - SPAN mode. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution	Bidder to comply with RFP terms.
363	Additional Point to be included	NA	Additional Point Anti APT - Sizing details required	Number of Internet Exit Points.	Bidder to comply with the RFP terms
364	Additional Point to be included	NA	Additional Point Anti APT - Sizing details required	Internet bandwidth in each internet gateway's.	Bidder to comply with the RFP terms
365	Additional Point to be included	NA	Additional Point Anti APT - Sizing details required	Number of Email Boxes & Number of email attachment per hour/ day.	Bidder to comply with the RFP terms
366	Additional Point to be included	Annexure-2, SIEM	SIEM	Can we get more information with respect to the use cases(from a Banking prspective); We suggest to make the platform more use-case-driven , which will give more proactive intelligence alerts & SOC team can take timely action, thereby reducing MTTR Also suggested to add cyber range in the scope. This will help to continuously assess & enhance the cyber posture of the Bank , check proactiovely varioius test scenarios and quantify the overall risk.	Bidder to comply with RFP terms.
367	Additional Point to be included	NA	SIEM	What is the number of target devices to be integrated with PIM?	Bidder to comply with the RFP terms
368	Additional Point to be included	NA	SIEM	Is there any web-based or thick-client based application need to be integrated with PIM?	Bidder to comply with the RFP terms
369	Additional Point to be included	NA	SIEM	Sensitive Fields in the logs should de-identified so that SOC analyst should not be able to see sensitive data. Only authorized users should be able to re-identify the sensitive data.	Bidder to comply with RFP terms.
370	Additional Point to be included	NA	SIEM	Every log event should be given a unique event id so that event can be tracked across multiple layers of SIEM.	Bidder to comply with RFP terms.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
371	Additional Point to be included	NA	SIEM	Proposed SIEM solution should have out of the box content for MITRE ATT&CK Framework. Default rules should be mapped with MITRE ATT&CK Framework Techniques and Tactics.	Bidder to comply with RFP terms.
372	Additional Point to be included	NA	SIEM	Proposed SIEM solution should have data science engine which enables analysts to do predictive analysis in reports.	Bidder to comply with RFP terms.
373	Additional Point to be included	NA	SIEM	The system should allow centralized management and reporting for various components from a single web based user interface.	Bidder to comply with RFP terms.
374	Additional Point to be included	NA	SIEM	The system should have interface to monitor health of the various components of solution and provide details like CPU usage, interface usage, disk status etc	Bidder to comply with RFP terms.
375	Additional Point to be included	NA	SIEM	SIEM solution should have OOB SOAR solution capability to reduce MTTD & MTTR	Bidder to comply with RFP terms.
376	Additional Point to be included	NA	PIM	What is the number of target devices to be integrated with PIM?	Bidder to comply with the RFP terms
377	Additional Point to be included	NA	PIM	Is there any web-based or thick-client based application need to be integrated with PIM?	Bidder to comply with the RFP terms
378	Additional Point to be included	NA	SIEM	Application control database must contain more than 6000 known applications.	Bidder to comply with RFP terms.
379	Additional Point to be included	NA	SIEM	The solution should have mechanisms to protect against spear phishing attacks	Bidder to comply with RFP terms.
380	Additional Point to be included	NA	NA	Proposed solution should be independent of existing Firewall, IPS, Proxy etc. so that in future if bank decide to replace any of these components solution should be able to work independently without a need of additional investment.	Bidder to comply with the RFP terms
381	Additional Point to be included	NA	NA	The solution should support concurrent execution of (but not limited to) " virtual machines so as to enable parallel analysis of multiple objects coming in the web traffic stream without impacting performance	Bidder to comply with the RFP terms
382	Additional Point to be included	NA	NA	Proposed Web APT solution should also have SSL Intercept capability (100% SSL traffic performance) to examine encrypted user bound traffic to detect threats (such as CnC traffic and data exfiltration) that attackers may hide in encrypted streams. If solution does not have native SSL capability, 3rd party SSL solution must be factored.	Bidder to comply with the RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
383	Additional Point to be included	NA	NA	The proposed solution should have the ability to be deployed in the following modes: - inline blocking - inline monitoring and, - SPAN mode. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution	Bidder to comply with the RFP terms
384	Clause not mentioned	NA	SIEM	Bidder understands that the new SIEM solution has to be implemented. Please confirm	Bidder to comply with RFP terms.
385	Clause not mentioned	NA	SIEM	Please confirm if the Bank will own the licenses of the SIEM tool OR they need to be owned by the Bidder	Bidder to comply with RFP terms.
386	Clause not mentioned	NA	SIEM	Bidder understands that bank expects on-premise solution for SIEM. Please confirm	Please refer to section 8 and Annexure-7 of the RFP for more details
387	Clause not mentioned	NA	SIEM	Please confirm if Bank is open for Cloud based SIEM	Bidder to comply with the RFP terms
388	Clause not mentioned	NA	SIEM	Please share the Incidents/Changes on SIEM in last 6 months with categorization on Critical, High and Medium	Bidder to comply with the RFP terms
389	Clause not mentioned	NA	SIEM	The Bidder understand that the existing ITSM tool will be leveraged for raising security incidents. Pls Confirm and provide the details of ITSM tool	Bidder is expected to provide incident management tool along with basic ticketing features as part of the total SIEM solution
390	Clause not mentioned	NA	SIEM	The Bidder understands that the Service Engineering support will be 8x5 Business hours and the Service Monitoring will be 24x7 via SIEM tool, Please confirm	Please refer to Annexure-6 of the RFP for more details
391	Clause not mentioned	NA	SIEM	Kindly confirm the reports and dashboards currently being generated and required from the Bidder	Bidder to comply with RFP terms.
392	Clause not mentioned	NA	SIEM	Please confirm the required SIEM architecture - Standalone in DC or HA (in DC) or Active-Passive / Active -Active (in DC & DR)	Please refer table-25 of Annexure-7 for more details
393	Clause not mentioned	NA	VM	What will be the frequency of conducting VA (Quarterly / half yearly/ yearly)	Please refer 8.9.3 Vulnerability Management Services
394	Clause not mentioned	NA	VM	Can VAPT be conducted from offshore as a service or a dedicated tool is required ?	Please refer 8.9.1 solution implementation
395	Clause not mentioned	NA	VM	What will be the duration of over all engagement one year/three year/five year?	Bidder to comply with the RFP terms

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
396	Clause not mentioned	NA	VM	How many different physical locations will be in scope of this activity? Is it possible to access all servers/devices in scope from central location and conduct the tests? If not Please share all the physical locations.	Bidder to comply with RFP terms.
397	Clause not mentioned	NA	VM	Is Customer looking for Application Security Assessment. If yes then please provide below details	Please refer 8.9.3 Vulnerability Management Services
398	Clause not mentioned	NA	VM	How many applications are in scope of assessment?	Refer Annexure 7 Scope of Work Table-29. The selected bidder will be provided with the details.
399	Clause not mentioned	NA	VM	Please provide the application stack: # of web applications? # of mobile applications? # of web services? # of thick client applications? # of other applications (please specify the details)?	Bank will provide the application details to the selected bidder
400	Clause not mentioned	NA	VM	Please mention the scanning frequency for: Penetration Testing (PT) = (Monthly/**Quarterly**/Half yearly/Annually) Static Code Review (SAST) = (Monthly/Quarterly/Half yearly/Annually) Dynamic Application Security Testing (DAST) = (Monthly/Quarterly/Half yearly/Annually)	Bidder to comply with the RFP terms
401	Clause not mentioned	NA	VM	Please confirm if the current security teams are located at multiple locations or centrally placed to manage the security devices	Bidder to comply with RFP terms.
402	Clause not mentioned	NA	VM	Is Bank open for onsite/ offshore support or complete onsite support is expected	Onsite support
403	Clause not mentioned	NA	Anti-APT	How many internet egress points are there in the network? The APT appliance will connect to the spam port of the core switch.	Bidder to comply with the RFP terms The selected bidder will be provided with the details.
404	Clause not mentioned	NA	Anti-APT	How much is the expected throughout of the traffic that will be passed through the appliance for inspection?	1. Bank Internet Throughput a. DC: 100 Mbps b. DR: 50 Mbps 2. Bank current LAN bandwidth utilization a. at DC Max Utilisation: 75% b. at DC Avg Utilisation: 40%
405	Clause not mentioned	NA	Anti-APT	Does the APT appliance have to monitor email traffic specifically?	Bidder to comply with RFP terms.
406	Clause not mentioned	NA	PIM	Are there any regulatory requirements those need to be complied ? If yes, please share the details	Bidder to comply with RFP terms.

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
407	Clause not mentioned	NA	PIM	Bidder understands that the scope for PIM is to implement the right solution and onboard the devices accordingly. Please confirm	Bidder to comply with RFP terms.
408	Clause not mentioned	NA	PIM	Bidder understands that application onboarding is not in scope. Please confirm.	Please refer Annexure 7 Scope of work
409	Clause not mentioned	NA	PIM	Have you done privileged account discovery anytime and do you have privileged account inventory? If yes pls share the account breakup details.	Bidder to comply with RFP terms.
410	Clause not mentioned	NA	PIM	Is vendor supposed to do privileged account discovery as a part of scope. Please confirm	Bidder to comply with RFP terms.
411	Clause not mentioned	NA	PIM	How many privileged accounts exists on the target servers? Please share the breakup.	Please refer to Annexure-7 of the RFP for more details Bank will share the detailed breakup of privileged accounts to the selected bidder
412	Clause not mentioned	NA	PIM	Is Bank open to do implemetation from Offshore location anywhere in India or it is completely through bangalore location. Please confirm	Implementation must be Onsite
413	Clause not mentioned	NA	PIM	Bidder is expected to provide license and AMC cost for 3 years, is this understanding correct?	Please refer RFP clause 56 and 57
414	Clause not mentioned	NA	PIM	We understand that there are 100 privilege users who will be accessing different devices. Is our understanding correct?	Please refer Annexure 7 Scope of work for Privilege Identity Management Solution
415	Clause not mentioned	NA	PIM	The bidders should also quote the additional cost in buckets of 20 Admin IDs.' as per the statement in RFP we understand that this will be additional 20 privilege user licenses. Is the bidder supposed to quote this for 1st year or 2nd year onwards	Bidder to comply with RFP terms.
416	Clause not mentioned	NA	PIM	Which different types of privileged account reports are generated? Who is reviewing the reports?	Bidder to comply with RFP terms.
417	Clause not mentioned	NA	PIM	What is the MFA solution currently implemeted in the Bank's environment	Bidder to comply with RFP terms.
418	Clause not mentioned	NA	PIM	What is the operational support window for the managed services?	Please refer to the RFP for more details related to SOC operations
419	Clause not mentioned	NA	PIM	Please provide details for the AD structure. Eg: Domains, Forests etc	Details to be provided to the selected bidder

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
420	Clause not mentioned	NA	PIM	Is there any defined PIM policy in place?	Bidder to comply with RFP terms.
421	Clause not mentioned	NA	PIM	Does all the privileged accounts have owners assigned to it?	Bidder to comply with RFP terms.
422	Clause not mentioned	NA	PIM	Are the privileged roles defined for each of the platforms? Eg: Windows, Unix etc	Yes
423	Clause not mentioned	NA	PIM	Are the privileged accounts recertified? If yes, how often and how it is done?	Bidder to comply with the RFP terms
424	Clause not mentioned	NA	PIM	Kindly share the information about key features expected to be implemented using PIM solution like: 1. SSO to endpoints without revealing password 2. Automatic Password Management 3. Real time monitoring & Session recording 4. least & Granular privilege command control 5. Secure management of SSH keys 6. Application to Application password management 7. Privilege Threat Anaytics	Please refer to Annexure-2 Technical requirements of the RFP for more details
425	Clause not mentioned	NA	PIM	How are the Databases being accessed and what kind of Database exists at present. (Eg: Oracle being accessed from TOAD)	The details will be shared with the selected bidder.
426	Clause not mentioned	NA	Infra	Please confirm if infra support is expected from Bidder post infra setup	Please refer to Annexure-7 for detailed scope of work.
427	Clause not mentioned	NA	Infra	Please confirm if hardware equipment for CSOC and for Security analysts(Desktops etc) has to be bought in by Bidder or Bank would be providing it	Bidder to comply with RFP terms.
428	Clause not mentioned	NA	Infra	What is the expection/outcome of the pre and post implementaion training	Bidder to comply with RFP terms.
429	Clause not mentioned	NA	Infra	Is Bidder expected to provide live-replication of logs for both DC/DR. Please confirm	Yes
430	Clause not mentioned	NA	General	What is the VPN solution that is currently being used.	Will be shared to the selected bidder
431	Clause not mentioned	NA	General	Please provide the details network device OEMs (Eg: Cisco etc)currently in the Bank's environment	Bank will provide the list of OEMs to the selected bidder

Sl. No.	Page No. of RFP	Clause No	RFP Clause	Bidder's Query	Banks Reply
432	Clause not mentioned	NA	General	What is the ITSM tool currenlty being used in the Bank's environement	It is requested from the bidder to provide bank the list of ITSM tools supported by the proposed solution along with supporting documents wherever applicable Bank is currently using CA tool.