S. No.	Section Name	Page No.	Point as stated in RFP	Description	SIDBI Response
1	2.21 point (h)	29	The bidder should submit bid on behalf of company they are representing and not in consortium or partnership with other vendors.	Kindly amend this clause as: The bidder should submit bid on behalf of company they are representing, bidder can have maximum of 1 consortium partner for this project	No change in RFP terms.
2	Annexure 8.2 Pre-Qualification Criteria for Bidder Point 3	104	The bidder should be involved in providing SOC/ CSOC in India for a minimum of three years as on 31.12.2018	Kindly amend the clause as: The bidder / consortium partner should be involved in providing SOC/ CSOC in India for a minimum of three years as on 31.12.2018	No change in RFP terms.
3	Annexure 8.2 Pre-Qualification Criteria for Bidder Point 6	105	The Bidder must have implemented /under implementation of Security Operations Center (SOC)/Cyber Security Operations Centre (CSOC) in at least 2 BFSI customers in India having project cost of 5 crores and above	Kindly amend the clause as: The Bidder/ consortium partner must have implemented /under implementation of Security Operations Center (SOC)/Cyber Security Operations Centre (CSOC) in at least 2 BFSI customers in India having project cost of 5 crores and above	No change in RFP terms.
4	Annexure 8.2 Pre-Qualification Criteria for Bidder Point 7	106	The bidder should have implemented SIEM in the BFSI institutions	Kindly amend the clause as: The bidder / consortium partner should have implemented SIEM in the BFSI institutions	No change in RFP terms.
5	Annexure 8.2 Pre-Qualification Criteria for Bidder Point 8	106	The bidder should have a minimum of 10 individuals with minimum two years of experience in implementation and management of Security Operations Centeror Cyber Security Operations Centre or both. All resources must be on the payroll of the bidder.	Kindly amend the clause as: The bidder / consortium partner should have a minimum of 10 individuals with minimum two years of experience in implementation and management of Security Operations Center or Cyber Security Operations Centre or both. All resources must be on the payroll of the bidder / consortium partner.	No change in RFP terms.
6	Annexure 11.4	163, Point number 10	The proposed solution should allow opening a Change Request for removing the Unused Rules and Covered rules directly from the analysis report for ease of operations. The removal of these rules should also be automatic irrespective of the firewall brand in case bank decides to procure change management module as well from the same OEM in near future.	Please confirm if SIDBI would like to procure the Firewall Change Management solution and whether that should be available from the day one during the Implementation?	The proposed solution should have mentioned capability.
7	Annexure 11.4	163, Point number 11	The proposed solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices	Please confirm total number of L3 Routers/Switches to build the network map automatically? Pls confirm total number of Physical and Virtual Firewall clusters/Pair?	The details will be shared with successful bidder.
8	Annexure 11.4	164, Point number 14	The proposed solution should have a change management capability and should support Bulk change request submission through Excel file	Please confirm if SIDBI needs Firewall change management capability also from the day one?	The proposed solution should have mentioned capability.
9	Annexure 11.4	165, Point number 26	The Proposed solution should have a scalability factor to discover and map the business applications and the associated logical connectivity with the underlying security policies. It should also be able to build the application flows based on the Firewall policies if required.	Please confirm what does scalability means? Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should be scalable and have mentioned capability if the bank requires in future.
10	Annexure 11.4	165, Point number 27	Solution should identify Blocked and allowed flows from an application perspective to enable application team to collaborate with the operations team	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
11	Annexure 11.4	165, Point number 29	The proposed solution should have a provision of decommissioning of business application. The decommissioning process should be fully automated and the rules should be removed automatically from the Firewalls only for that application which needs to be decommissioned. The system should also identify those rules which cannot be removed as those could be linked to other applications.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
12	Annexure 11.4	165, Point number 30	The proposed solution should be application centric and have a provision for server migration process. The process should be fully automated and should specify the inline applications and their logical connectivity which requires changes. The proposed system should even provision the necessary rules on the FW's automatically.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm the number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.

13	Annexure 11.4	165, Point number 31	The solution should provide an ability to verify the impact on business applications if the inline FW is down or a specific policy on the FW is blocking the application traffic	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
14	Annexure 11.4	165, Point number 32	The proposed solution should have a capability to map the Firewall configuration risks with the inline business applications. It should present the risks in the overall application context.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
15	3.3 Current Information Technology Setup	Page 33, Point A	Data Centre and DR Site	Please confirm if the solution is required in HA-DR architecture or only at DC as a standalone solution?	Please refer Section 4 Scope of Work of RFP.
16	Annexure 11.1 Security Information and Event Management	142	#1. The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope	As per our understanding "Propose solution should be appliance based and separate hardware for collection, loging and correlation". Is our understanding correct?	The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module.
17	Annexure 11.1 Security Information and Event Management	142	#6. Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	As per our understanding "Propose hardware should be capable to handle sustained 20,000 EPS along with storage from Day 1". Is our understanding correct?	The bidder has to provide SIEM license for 10000 EPS and storage for minimum 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
18	Annexure 11.1 Security Information and Event Management	144	#29. The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis.	Please share Network Throughput to size Packet Capture solution. Ex: " Packet capture solution should support 1 Gbps traffic along with 4 network ports (2 X 1 Gbps + 2 X 10 Gbps)	The bank currently has network throughput of 10 Gbps traffic.
19	Annexure 11.1 Security Information and Event Management	147	#77. The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities	As per our understanding this point relate to investigate the incidents. Need clarity on report as report can be generate as per pending incidents and analyse can be done on pending mitigation activities. IS our understanding correct	The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities
20	Annexure 11.1 Security Information and Event Management	148	#98. System should have capacity to maintain the logs for 90 days on Tier I storage and older logs should be archived on Tier II storage and Tier 3 storage	As per our understanding storage should be sized for 20,000 EPS from Day 1. Is our understanding correct?	The bidder has to provide storage for minimum 10000 EPS from day 1 and same appliance should support / scalable upto 20000 EPS.
21	44	4.5 - H	The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement	License , Hardware & software should be sized for 2000 devices from day 1? 1 Device = 1 IP , Our Assumption is correct?	The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement
22	44	4.5 - i	The Bank has offices at around 80 locations in addition to the DC and DR. Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, Bank has placed order for implementation of SD-WAN based IP MPLS network. The routers at the locations will be replaced with SD-WAN CPEs. The proposed solution should be able to capture logs from the CPE's installed at the locations. The Bidder's proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period	Please share the SD-WAN vendor details. What is the outcome/usecases bank are expecting with integrating SD-WAN solution? The proposed solution should be able to capture logs from the CPE's installed at the locations.----- Ideally Logs Capture is the feature of SIEM/Syslog solution , Request you to clarify, what are the expected outcome from NAC?	The vendor for SD-WAN currently is Sify. The usecase expected here is visibility and profiling.
23	50	z	OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.	Bidder will be the implementation & sustainance partner for bank , Request you to repharse it "Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation. "	The Bidder would be the single point of contact. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.

24	166	12	The solution should support existing third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM.	Please highlight the use case wrt all third party hardware/software. For exact boq sizing vendor details are must, Integration outcome is require from day 1? What all use cases/Outcome bank is expecting with integrating all the tools?	The hardware/software/devices/appliances are from the leading manufactures. The details will be shared with successful bidders.
25	167	30	The NAC Solution should support agentless , agent base & Desolvable agent mode	It is important for bank to check posture complaince with all the deployement mode, request you to repharse it as " The NAC Solution should support agentless , agent base & Desolvable agent mode for all the feature listed in technical compliance sheet (i.e discovery , profiling , posturing , access control & remediation.)"	No change in RFP terms
26			Additional Query	Provide Network Infrastructure details (Like Total Number of switches , Routers, Wireless , Firewall etc)	Refer Annexure 11.7. The further details will be shared with the successful bidder.
27			Point Need to be added	For Bank there are many IOT(Printers , Scanners , IP phone , IP camera , cheque scanning machine) devices connecting on to the enterprise network , its very important to include IOT posture assesment , The solution should be able to identify all network devices such as routers, switches, IOT's devices using factory default or Weak/common credentials as part of IOT Risk Assessment.	This is to be taken care in Vulnerability Assessment and Penetration Testing services.
28			Point Need to be added	The NAC solution should support bank existing network infrastructure i.e Managed & unmanaged swiches to block or limit the non-complied and rough devices behind that.	No change in RFP terms
29			Point Need to be added	The solution should provide complete inventory of applications, processes, Services and open ports on all the endpoint.	No change in RFP terms
30			Point Need to be added	The solution should provide visibility into IPv6 enabled endpoints.	Separate clause has been added. Please refer to Corrigendum - 2.
31	Service Level Agreement & Liquidated Damages	95	b) In case, if there is delay in delivery of the hardware & software, installation of the security solutions and associated hardware, software and software licenses, as given in commercial bid, beyond the schedule given in Section 4.10 from date of issue of PO, then LD at the rate of 1% per week of the cost quoted against each of respective item as mentioned in Commercial Bid for items not delivered will be levied per week or part thereof (on pro rata basis for the no. of days) and deducted against bills submitted.	The penalty is too high. Kindly consider it 0.5% per week	No change in RFP terms
32	Service Level Agreement & Liquidated Damages	95	c) The integration of all the security solutions with SIEM should be completed within a period as mentioned in the section 4.10 from the date of issue of PO. In case of delay in integration beyond three months, LD at the rate of 1% per month of the cost quoted against SIEM as mentioned in Commercial Bid will be levied per month for the no of days of delay (on pro rata basis for the no. of days) and deducted against bills submitted.	The penalty is too high. Kindly consider it 0.5% per month	No change in RFP terms
33	7.2. Liquidated damages for not maintaining uptime	96	1. CSOC Operations Failure including any device (hardware / software) failure resulting in failure of CSOC operations	Whether given SLA is for the complete solution failed or any device failed?	The SLAs are for device failures, please refer section 7 of the RFP
34	7.2. Liquidated damages for not maintaining uptime	96	97% to 99%- 1% of Total CSOC Monitoring and Operations cost for each failure	The penalty is very high, kindly relax it up to 0.5%	No change in RFP terms
35			95% to 96.99% - 5% of Total CSOC Monitoring and Operations cost for each failure	The penalty is very high, kindly relax it up to 3%	No change in RFP terms
36			Less than 95%- 10% of Total CSOC Monitoring and Operations cost for each failure	The penalty is very high, kindly relax it up to 7%	No change in RFP terms
37	7.3. SLAs & Liquidity Damages for CSOC Operations	101	Advisories within 12 hours of new global threats & vulnerabilities disclosures.	This is OEM dependent point, request you to relax it.	No change in RFP terms
38	4.10. Implementation Phases and Timelines	57	Installation & Configuration of SIEM and other Security Tools / Solutions	Kindly consider 12 weeks time from acceptance of PO	Refer to Corrigendum - 2
39	4.10. Implementation Phases and Timelines	57	User Acceptance Test (UAT) and making the CSOC operational	14 weeks time to complete the entire project would be difficult, kindly consider at least 18 weeks of time	Refer to Corrigendum - 2

40	6.13. Terms of Payment and Payment Milestones	72	p) The payment milestones are defined as below: 50% on Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS 20% on Post UAT signoff (Phase-1) 30% on Post project signoff (Phase-2)	Request to revise the clause as below for healthy cash flow of the project and avoid un-necessary incurring of interests: p) The payment milestones are defined as below: 70% on Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS 20% on Post UAT signoff (Phase-1) 10% on Post project signoff (Phase-2) or against BG of equivalent amount	No change in RFP terms
41	4.10. Implementation Phases and Timelines	57	Delivery of CSOC Hardware / Software and licenses and resources 4 - 6 weeks from acceptance of PO	Request to dilute the criteria as: Delivery of CSOC Hardware / Software and licenses and resources 8 weeks from acceptance of PO	Refer to Corrigendum - 2
42	5.2. Technical Evaluation	58	c) Commercial Bid will be opened only for those Bidders who score minimum of 80% in Technical Evaluation (RSTech)	Request to kindly dilute the clause as: c) Commercial Bid will be opened only for those Bidders who score minimum of 70% in Technical Evaluation (RSTech) 80 % evelaustion is far above the normal industrial standards and would be very stringent.	No change in RFP terms
43	Annexure 8.2 Pre-Qualification Criteria for Bidder	105	a. The Bidder must have implemented / under implementation of Security Operations Center (SOC) / Cyber Security Operations Centre (CSOC) in at least 2 BFSI customers in India having project cost of 5 crores and above b. The project cost for these implementations should be as below: i. one project cost should be 15 crores and above and........	Request to include BSFI/ PSU customers as below: a. The Bidder must have implemented / under implementation of Security Operations Center (SOC) / Cyber Security Operations Centre (CSOC) in at least 2 BFSI/PSU customers in India having project cost of 5 crores and above b. The project cost for these implementations should be as below: i. one project cost should be 15 crores and above and........	No change in RFP terms
44	Section 4.8.6 Monitoring	54	DC Operator (System Administrator) Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai	Wipro assumes that all the resources for IT infra mangement of in-scope services mentioned in RFP would be based out of DC site, Navi Mumbai	The CSOC operations will be carried out from Chennai. However one resource is required at Mumbai DC site.
45	Section 4.8.6 Monitoring	52	CSOC activities and events from each solution and devices already present in the bank's environment on a 12*6 basis (8 am to 8 pm) basis and suggest/ take appropriate action on an on-going basis.	Wipro assumes that coverage/ service window for DC Operation (IT Infra management for in-scope services of this RFP) will also be on 12*6 basis (8 am to 8 pm). However IT Infra Monitoring will be 24*7 basis. Please confirm.	The Bank is looking for 12*6 monitoring. The bidder has to maintain SLAs as per section 7 of the RFP.
46	Section 4.8.6 Monitoring	54	DC Operator (System Administrator) Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai	Please confirm if SI needs to provide "Hands and Feet Support" for DC and DR hardware. If yes, please provide the location (pin codes) and service window for the same along with the SLA.	One resource is required to be onsite at Data Centre on 12*6 basis. Please refer Section 4 Scope of Work of the RFP.
47	Section 4.8.6 Monitoring	54	DC Operator (System Administrator) Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai	Please confirm the DC/DR drill frequency	The details will be shared with selected bidders.
48	Section 4.8.6 Monitoring	54	DC Operator (System Administrator) Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai	Wipro assumes that all the infra (desktops / workstations, landline, seating space amongst others) will be provided by SIDBI. Kindly confirm	Bidder needs to provide all infrastructure. Please refer section 4 Scope of the work of RFP.
49	Section 4.8.6 Monitoring	54	DC Operator (System Administrator) Managing and administrating entire infrastructure (server, storage, network devices, etc.) of CSOC operations at DC Site, Navi Mumbai	Wipro assumes that it can sub-contract to its third party vendors for IT Infrastructure Managed Support Services.	Sub-contracting is not permitted under this RFP.

50	Section 7.3 SLAs & Liquidity Damages for CSOC	98	NA	SLA measurement shall exclude following • Scheduled downtime on account of preventive maintenance • Downtime caused because of the inadvertent mistake by Third party service provider (under contract with customer) or customer's personnel. This will include configuration changes made by the customer personnel affecting expected performance without notifying Wipro. Time taken for all Incidents that require Change Management Process and IT/ Business Management approval will have excluded from total resolution time. • SLA's will not be measured during any natural calamities / disasters, hardware failures (vendor dependency) and planned outages / maintenance etc., in such scenarios the services will be delivered on best effort basis • Limitation of OEM Hardware / IOS / Firmware and Bugs without resolutions • Issues raised due to Capacity, Availability, Component Failure Impact Analysis (CFIA), Failure Modes and Effect Analysis (FMEA) issues of the landscape highlighted by Wipro in this format or in Risk Register, and in event of action pending with "Customer" Issues related to Network Link service provider issues like	No change in RFP terms
51	Section 4, Scope of Work	38	NA	Wipro shall not be liable for Data Loss due to any circumstances. Such data shall be restored through reasonable efforts basis based on the technology available. Backed up data and upon specific customer approval, shall be recovered through specialized low level data recovery agency. Identification of such a vendor will be customer's responsibility. Cost for such data recovery to be provided by customer. Kindly confirm	No change in RFP terms
52	4. Scope of Work	38	post warranty maintenance support	need the clarity on 4th and 5th year AMC	The bidder has to provide cost of AMC for 4th and 5th year as part of commercial bid.
53	4.1. Security Information and Event Management A. Solution Implementation:	39	j) The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site.	Our understanding is bidder to provide the required bandwdith details to bank for repication for DC and DR site.	The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder. If required, SIDBI will enter into a tri-party agreement with the bidder and service provider for obtaining P2P link. The uptime of this link will be the responsibility of the service provider providing P2P link.
54	4.1. Security Information and Event Management C. Log collection		located at the geographically dispersed location should be collected	details of geographically dispersed location	Majority of the devices are located in DC and DR of the bank.
55	4.5. Network Access Control (NAC)		Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement.	Please provide the no of licensing count required on day 1 and YoY the addditional licensing of 2000 need to be factored across 3 Years .	The bidder has to factor the solution for 2000 users from day 1.
56	4.8. Other General Requirement 4.8.1. Hardware, Software and Network Connectivity		h) Bidder should consider sizing as part of integration of additional devices during the contract period.	Please provide the count of devices that need to be intergrated across the tenure peroid	Please refer to annexure 11.7 of the RFP.
57	4.8. Other General Requirement 4.8.1. Hardware, Software and Network Connectivity		i) The network connectivity between SIDBI offices, Data Centre site and Disaster Recovery Site will be provided by the bank. The bidder will be responsible for any other network connectivity required for CSOC operations and P2P link for replication of logs of SIEM collectors in DC and DR.	Please provide the connectivity between branches to DC for Log collection	All the SIDBI branches are connected to DC through MPLS link.
58	4.8. Other General Requirement 4.8.3. Implementation & Integration		a) Implementation should comply with the SIDBI Information Security Policy, SIDBI Cyber Security Policy and RBI Guidelines such as Cyber Security Guidelines, Gopal Krishna Committee guidelines, Localization of Payment Storage guidelines etc. and as specified from time to time.	Request bank to provide the Guidelines, polices and procedure that bidder need to adhere to.	The bidder has to support the CSOC solutions for the Bank against all the compliance standards maintained by the Bank. The required set of policies and procedures will be shared with successful bidder.

59	4.8. Other General Requirement 4.8.3. Implementation & Integration		c) A comprehensive strategy should be provided by the Bidder on implementing the end to end CSOC solution within 7 days of issuance of Purchase Order (PO).	The Timelines to be changed from 7 days to 15-20 Days	Refer to Corrigendum - 2
60	4.8. Other General Requirement 4.8.3. Implementation & Integration		h) The bidders needs to provide warranty for entire 3 years at the start of contract period and warranty period will commence from the acceptance date of phase-1 UAT signoff from Bank.	the warranty starts from the date of license issuance	No change in RFP terms
61	4.8. Other General Requirement 4.8.3. Implementation & Integration		i) In addition, the bidder is responsible for impact assessment and modification of SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations. Bidder should consider sizing as part of integration of additional devices during the contract period. SIDBI will not be responsible to pay for any further hardware cost.	integration of additional devices during the contract period. SIDBI will not be responsible to pay for any further hardware cost.	No change in RFP terms
62	4.10. Implementation Phases and Timelines		Integration of SIEM with other Security Tools / Solutions under CSOC	Request Bank to increase the timeline from 11 Weeks to 16 Weeks as there is dependency with Network team and End User availability across locations	Refer to Corrigendum - 2
63	Annexure 11.1 Security Information and Event Management	143	The proposed solution should integrate with other security solutions, such as IPS/IDS, Proxy, Anti-virus etc.	Request Bank to provide the list of devices and Application details that need t be integrated with SIEM solution	Refer to Annexure 11.7 of the RFP.
64	Annexure 11.1 Security Information and Event Management		The proposed solution should have out of the box rules for IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, databases and standard applications etc.	Please provide the location wise split for the devices and also please provide the flavor for databases and Applications	Majority of the devices are located in DC and DR of the bank. The hardware / software / devices / appliances are from the leading manufactures. The details will be shared with successful bidders.
65	Annexure 11.1 Security Information and Event Management	149	Integrate with existing helpdesk/ incident management tools	Please provide the existing Helpdesk & Incident Maangement tool details	The bidder has to propose Incident Management tool to identify the incidents generated from SIEM.
66	Annexure 11.1 Security Information and Event Management	150	The offered solution should be able to collect, correlate and analyze logs from various devices located at different locations of SIDBI, without any additional cost implication on SIDBI. The locations covered are Data Center, Navi Mumbai and DR Chennai. However it must be possible to include devices located at other locations of SIDBI without any significant changes in implementation.	Please provide the location and their connectivty details with centralzed DC and DR site	Majority of the devices are located and connected to DC and DR of the bank. The DC is located at Navi Mumbai and DR site is located at Chennai.
67	4.5. Network Access Control (NAC)	43	Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba	Whether the Swiches hosted across locations are managble or non Manageable swicthes	The switches hosted across are manageable switches.
68	4.5. Network Access Control (NAC)	43		Whether the endpoints conecting over a network are based on Static IP / DHCP IP	Endpoints connected over network are based on Static IP.
69	4.5. Network Access Control (NAC)	43		Are devices such as printers, scanners and VOIP devices in scope as well, do you have inventory for the same	NAC needs to be implemented only for endpoints.
70	4.5. Network Access Control (NAC)	43		Are you considering 802.1x Authentication only for Wired or wireless as well. If yes then please elaborate: a) Do you have centralized or distributed WLAN deployment b) What are the Make and model of wireless devices c) Do you have single domain or multiple domain	The proposed solution should support both Wired or Wireless. However currently, there is no Wireless setup.
71	4.5. Network Access Control (NAC)	43	Existing Environmental details	Whether clinet have SCCM tool within their premises for pushing the agent from a centrzlided sie	Please refer to point (j) of section 4.5 of the RFP.
72	4.5. Network Access Control (NAC)	43	What are the existing incident management processes for NAC alerts	Please elaborate on the endpoint security measures which have been implemented e.g. AV Anti spyware, Windows firewall etc	Please refer section 3.3 "Current IT Infrastructure" of the RFP.
73	4.3. Anti-Advance Persistent Threat (APT)	42	a) Bidder should install and configure Anti - APT solution to protect against web and email attacks.	Please provide existing Web proxy and Mail Gateways details. Whether Web Proxy solution hsoted at a centralzied site or distributed.	Please refer section 3.3 "Current IT Infrastructure" of the RFP. The Web proxy and mail gateway are hosted at centralized site. Further details will be shared with successful bidder.
74	4.4. Firewall Analyzer	43	Integration of 10 firewalls with Firewall Analyzer	Whether the Firewall hosted in SIDBI site are working as standalone device or placed in cluster.	Majority of the firewalls are hosted in HA mode.
75	VAPT Information and Remediation Services	44	VAPT Information and Remediation Services	The required compute for implementing Vulnerabilty assememeht tool will be provided by client or bidder need to provision the require hardware.	The bidder has to bring in their own tools and hardware for VAPT services. However, the bidder needs to make available all required resources at time of VAPT.

76	General Query			Please specify the RPO and RTO. Also do confirm if we need to propose DR automation tool.	The CSOC operations need to maintain SLA and uptime as per Section 7 of the RFP. The RPO should be for 60 minutes. Yes
77	4.8.1. Hardware, Software and Network Connectivity	46	e) The bidder needs to propose only Veritas backup solution for backups.	Is veritas the existing solution for backup. If so the implementation of the same would be done by the existing team or the bidder	Yes, the existing solution for backup is Veritas. The bidder needs to propose only Veritas backup solution for backups. The Bidder will be responsible for implementing the solution for backup and carrying out backups and transportation to offsite. Please refer to Section 4 Scope of work of RFP.
78	4.8.1. Hardware, Software and Network Connectivity	47	g) There should be three separate environments: Development, Test (UAT), and Production (DC-DR). The environments must be configured on a separate physical servers. The Development environment should have at least 20% and Test (UAT) environments should have at least 50% of the configuration of the Production environment quoted by the Bidder.	As mentioned that separate servers are required for Dev, UAT and Production. Please confirm if we need to factor separate storage for different environments or the same storage will suffice	The bidder can use the same storage once the development and UAT phase is completed. However, all the updates/patches/fixes need to be tested in UAT before pushing these to production environment.
79	4.5 NAC	44	Bidder should perform any OS upgrade on the network switches if required.	Please provide the make and models of switches for which OS upgrade needs to be done. Also specify the quantity of switches.	The hardware / software / devices / appliances are from the leading manufactures. Further details will be shared with successful bidder.
80	4.1 SIEM A-Solution Implementation	39	m. Bidder will also supply all the necessary Switches / cables / connectors / hardware /software etc. for integration of the components supplied for CSOC. Bank will supply only the Rack space, power and a network point in the Server room	Please specify the count of switches / tech specs and preferred make /model.	The bidder has to factor all the necessary Switches / cables / connectors / hardware /software etc. for integration of the components supplied for CSOC. All the supplied components should be from leading manufacturers.
81	General Query		Cabling	is the cabling in bidders scope? Does this include only patch cords or rack to rack cabling also?	Inter-rack cabling will be the responsibility of the bank.
82	General Query			Please specify the RPO and RTO. Also do confirm if we need to propose DR automation tool.	The CSOC operations need to maintain SLA and uptime as per Section 7 of the RFP. The RPO should be for 60 minutes. Yes
83	4.8.1. Hardware, Software and Network Connectivity	46	e) The bidder needs to propose only Veritas backup solution for backups.	Is veritas the existing solution for backup. If so the implementation of the same would be done by the existing team or the bidder	Yes, the existing solution for backup is Veritas. The Bidder will be responsible for implementing the solution for backup and carrying out backups and transportation to offsite. Please refer to Section 4 Scope of work of RFP.
84	4.8.1. Hardware, Software and Network Connectivity	47	g) There should be three separate environments: Development, Test (UAT), and Production (DC-DR). The environments must be configured on a separate physical servers. The Development environment should have at least 20% and Test (UAT) environments should have at least 50% of the configuration of the Production environment quoted by the Bidder.	As mentioned that separate servers are required for Dev, UAT and Production. Please confirm if we need to factor separate storage for different environments or the same storage will suffice	The bidder can use the same storage once the development and UAT phase is completed. However, all the updates/patches/fixes need to be tested in UAT before pushing these to production environment.
85	Preface	13	This Request for Proposal document ('RFP document' or RFP) has been prepared solely for the purpose to outsource the Implementation and Management of Cyber Security Operations Center (CSOC), which includes the Maintenance and Support for a period of three years and extendable for a further duration of maximum two years at the discretion of the Bank under THREE (3) Bid System viz.	This Request for Proposal document ('RFP document' or RFP) has been prepared solely for the purpose to outsource the Implementation and Management of Cyber Security Operations Center (CSOC), which includes the Maintenance and Support for a period of three years and extendable for a further duration of maximum two years at mutual discussion between the Parties ~~the discretion of the Bank~~ under THREE (3) Bid System viz.	No Change in RFP terms.

86	Information Provided	13	The RFP document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with SIDBI. Neither SIDBI nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document. Neither SIDBI nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.	The RFP document contains statements derived from information that is believed to be relevant at the date but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with SIDBI. ~~Neither SIDBI nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied, as to the accuracy or completeness of any information or statement given or made in this document. Neither SIDBI nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.~~	No Change in RFP terms.
87	Receiving of RFP Response	19	The Recipient shall be deemed to have licensed and granted all rights to the Bank to reproduce the whole or any portion of their submission for the purpose of evaluation and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right of the Recipient that may subsist in the submission or accompanying documents.	~~The Recipient shall be deemed to have licensed and granted all rights to the Bank to reproduce the whole or any portion of their submission for the purpose of evaluation and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right of the Recipient that may subsist in the submission or accompanying documents.~~	No Change in RFP terms.
88	Rules for Responding to the RFP	20	n) The Bidders shall adhere to the terms of this RFP document and shall not deviate from the same. If the Bidders have absolutely genuine issues only then should they provide their nature of non-compliance to the same in the format provided separately with this RFP. The Bank reserves its right to not to accept such deviations to the Tender terms, in its sole and absolute discretion, and shall not be obliged to furnish any reason for exercising such right.	If the bidder deviates for genuine issues, will the EMD of the bidder to forfeited?	No Change in RFP terms.
89	Period of Validity of Bids	22	As per RFP	Prices and other terms offered by Bidders must be firm for an acceptance period of ~~nine (9)~~ one (1) months from last date for submission of bids	No Change in RFP terms.
90	Responsibility of the Bidder	29	As per RFP	e) The selected bidder will provide access to the Bank or auditors/consultants engaged by / representing the Bank for inspection / audit of its CSOC operations (except internal cost record) for any compliance or regulatory requirements. The selected bidder will facilitate and provide additional support during all audits conducted by the bank as part of contract period. The selected Bidder shall not bear the cost of such inspection/ audit by the Bank. i) The Bidder represents and acknowledges to the Bank that it possesses necessary experience, expertise and ability to undertake and fulfill its obligations, under all phases involved in the performance of the provisions of this RFP. The Bidder represents that all software and hardware to be supplied in response to this RFP shall meet the requirement of the solution proposed by the Bidder. The Bidder shall be required to independently arrive at a solution, which is suitable for the Bank, after taking into consideration the effort estimated for implementation of the same. ~~If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or~~	No Change in RFP terms.

91	Objective	31	Bank expect Service provider to provide fullfledged Services including but not limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies. The Bank has plans .... The bidder is expected to do following but not limited to:	Bank expect Service provider to provide fullfledged Services ~~including but not~~ limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities related to or connected to the Information Technology / Cyber security solutions, devices & technologies. The Bank has plans .... The bidder is expected to do following ~~but not limited to~~:	No Change in RFP terms.
92	Scope of Work	38	As per RFP	The Scope of work for Cyber-Security Operation Centre (CSOC) ~~including but not limited~~ to design, supply, configuration, implementation, customization, integrations, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support and any other activities related to or connected to the IT security, Security solutions, devices and technologies.	No Change in RFP terms.
93	Training	47	The bidder is required to provide all trainees with detailed training material and 2 additional copies to the bank for each solution as per the scope of work of the bank. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution. f) All out of pocket expenses related to training shall be borne by the selected bidder.	Bank to clarify on the counts of tarining manuals required. Also, f) All out of pocket expenses related to training shall be ~~borne by~~ reimbursed to the selected bidder on actuals.	No Change in RFP terms.
94	Implementation & Integration	48	i) In addition, the bidder is responsible for impact assessment and modification of SOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations. Bidder should consider sizing as part of integration of additional devices during the contract period. SIDBI will not be responsible to pay for any further hardware cost. j) The bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure. SIDBI will not be responsible to pay for any additional cost required as part of additional capacity required. k) The Bidder should provide the latest version of the Solution. The bidder would be responsible for replacing the out-of-support, out-of-service, end-of-life, undersized, infrastructure elements at no extra cost to the bank during the contract period. Replacement to be done before 15 days from due of date of the product/service. l) The support for all the solutions proposed should be provided for the contract period. Whereas free upgrade should be provided for all solutions if the end of life occurs within the period of contract with bank. The Updates/ Upgrades for medium and low should be implemented within 3 months of release of the same. For critical and high upgrades / updates, implementation to be implemented within 1 months of release. m) All the solutions supplied as part of this RFP	t) Development and implementation of processes for management and operation of the CSOC including ~~(but not limited to)~~ the following processes:	No Change in RFP terms.
95	4.8.5. System Integration Testing (SIT) and User Acceptance Testing (UAT)	52	As per RFP	f) The Bank will accept the solution on ~~satisfactory~~ completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the Bank. The solution shall be deemed to be accepted if the Bank fails to inspect the solution within 15 days from the date of intimation of the same by the Bidder. g) In case of discrepancy in facilities /services provided, the Bank reserves the right to cancel the entire contract after giving a cure period of 30 days.	No Change in RFP terms.
96	Continuous Improvement	55	As per RFP	d) Bidder needs to update all solutions and Cyber Security Operations Centre (CSOC) based on any new regulations and RBI guidelines as a change requent at an additional cost.	No Change in RFP terms.

97	Period of Contract	55	As per RFP	a) Bidder is required to provide the services for a period of 3 years extendable for a further duration of maximum two years after mutual discussions between the parties ~~at the discretion of the Bank~~ on the same terms and conditions. e) In case of termination of contract / end of contract period, bidder has to provide extended services, with the rates discussed mutually ~~mentioned as of last year~~. This extension of services to be provided till procurement of next solution / till 1 year, with ~~same~~ mutually discussed terms and conditions.	No Change in RFP terms.
98	Evaluation Methodology	58	The selected bidder will be entrusted with end-to-end responsibility of management of Implementation and Management of Cyber Security Operations Center (CSOC) for the period of three (03) years which can be extended for a further duration of maximum two years at the discretion of the Bank.	The selected bidder will be entrusted with end-to-end responsibility of management of Implementation and Management of Cyber Security Operations Center (CSOC) for the period of three (03) years which can be extended for a further duration of maximum two years with a consent of both parties ~~at the discretion of the Bank~~.	No Change in RFP terms.
99	Pre-Qualification Criteria	58	As per RFP	b) The Bidder is required to provide factually correct responses to the RFP. Adequate justification for the response (including the technical and other requirements) should be provided as part of the response. In case the Bank finds any response to be inadequate, the Bank has the right to ask for additional explanation/ justification. In the event of any discrepancy in the response submitted by the Bidder, the Bank reserves the right to disqualify~~/ blacklist~~ the Bidder and the OEM.	No Change in RFP terms.
100	Issue of purchase order	63	As per RFP	Request addition of "PO shall – (a) Be solely governed by the terms and conditions of the Contract mutually signed and agreed (b) Make an express reference to the Contract It is also clarified that no pre-printed terms and conditions mentioned in the Procuring Document shall apply to the successful bidder."	No Change in RFP terms.
101	Bid Security / Earnest Money Deposit (EMD	64	e) The amount of Earnest money deposit (EMD) would be forfeited in the following scenarios: i) In case the Bidder withdraws the bid prior to validity period of the bid for any reason whatsoever;.................................. iv) In case the successful Bidder fails to provide the Performance Bank guarantee within ONE month from the date of issue of Purchase Order by the Bank. Besides forfeiting the EMD, the Bank may ban the bidder from subsequent bidding for a period of not less than 3 years.	e) The amount of Earnest money deposit (EMD) would be forfeited in the following scenarios: i) ~~In case the Bidder withdraws the bid prior to validity period of the bid for any reason whatsoever~~;.................................. iv) ~~In case the successful Bidder fails to provide the Performance Bank guarantee within ONE month from the date of issue of Purchase Order by the Bank. Besides forfeiting the EMD, the Bank may ban the bidder from subsequent bidding for a period of not less than 3 years.~~	No Change in RFP terms.

102	Performance Bank Guarantee (PBG)	64	b) In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder. d) The Performance Bank Guarantee would be returned to the successful Bidder after the expiry or termination of the contract plus 90 days on satisfaction of the Bank that there are no dues recoverable from the successful Bidder. h) Time shall be the essence of the contract / order, therefore, no extension of time is anticipated, but if untoward or extraordinary circumstances should arise beyond the control of the Bidder, which in the opinion of SIDBI should entitle the Bidder to a reasonable extension of time, such extension may be considered by SIDBI at its sole and absolute discretion, however such extension shall not operate to relieve the Bidder of any of its obligations. SIDBI shall not be liable for any extra financial commitment due to such extension of time. In case of any such extension, the Bidder would be required to extend the validity period of the performance guarantee accordingly.	b) In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee with~~out~~ notice or right of demur to the Bidder of thirty (30) working days. h) ~~Time shall be the essence of the contract / order, therefore,~~ no extension of time is anticipated, but if untoward or extraordinary circumstances should arise beyond the control of the Bidder, which in the opinion of SIDBI should entitle the Bidder to a reasonable extension of time, such extension may be considered by SIDBI at its sole and absolute discretion, however such extension shall not operate to relieve the Bidder of any of its obligations. SIDBI shall not be liable for any extra financial commitment due to such extension of time. In case of any such extension, the Bidder would be required to extend the validity period of the performance guarantee accordingly.	No Change in RFP terms.
103	Forfeiture of performance security	66	b) In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the Bidder.	b) In the event of non-performance of obligation or failure to meet terms of this RFP / Contract, the Bank shall be entitled to invoke the performance guarantee with~~out~~ notice or right of demur to the Bidder of thirty (30) working days.	No Change in RFP terms.
104	Commercial Bid	68	c) Tax -The prices quoted would include all costs including applicable taxes like GST, custom duties, transportation, out of pocket expenses, lodging and boarding expenses, etc., that need to be incurred (at current rate). No additional cost whatsoever would be paid	c) Tax -The prices quoted would ~~include~~ exclude all costs including applicable taxes like GST, custom duties, transportation, out of pocket expenses, lodging and boarding expenses, etc., that need to be incurred (at current rate). ~~No additional cost whatsoever would be paid~~ Tranportation, out of pocket expenses, lodging and boarding expenses shall be reimbursed by the customer on Actuals.	No Change in RFP terms.
105	Service Delivery	69	e) Time is the essence of this RFP / Contract to be entered with the Successful Bidder, therefore, the Bidder must strictly adhere to the delivery schedule of the manpower and services identified in their proposal. Failure to do so will be considered as breach of the terms and conditions of the contract. g) SIDBI reserves the right to reduce resources anytime during the contract period without assigning any reason thereof, with a prior written notice of 30 days. Payment of such resources shall be made on pro-rata basis till the date of stopping.	e) ~~Time is the essence of this RFP / Contract to be entered with the Successful Bidder, therefore, tThe~~ Bidder must strictly adhere to the delivery schedule of the manpower and services identified in their proposal. Failure to do so will be considered as breach of the terms and conditions of the contract. ~~g) SIDBI reserves the right to reduce resources anytime during the contract period without assigning any reason thereof, with a prior written notice of 30 days. Payment of such resources shall be made on pro-rata basis till the date of stopping.~~	No Change in RFP terms.
106	Ownership of Deliverables	69	As per RFP	a) The selected Bidder, who will be awarded the contract, will hold ownership of its delivery of the services under the contract and be responsible for the services delivered. All the deliverables as per the scope of this RfP will become the property of the Bank on the payment of relevant service fees. To be added: No intellectual property rights of any nature shall be transferred from one party to the other in the course of performing any obligations or otherwise under this agreement. For the avoidance of doubt, Bidder may use certain tools, processes or methodologies of its own in performing the Services. Ownership of all intellectual property rights and any other rights in these shall vest with Bidder, and no rights shall be deemed to have accrued to the Customer.	No Change in RFP terms.
107	6.12. Expenses	70	It may be noted that SIDBI will not pay any additional amount separately towards travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses or any other fees / charges.	Request to remove the clause	No Change in RFP terms.

108	6.13. Terms of Payment and Payment Milestones	71	n) The Price offered by the Bidder to the Bank must be in Indian Rupees and payments will be made to the Bidder in Indian Rupee only. The costs should be inclusive of duties, insurance, freight, charges of road permit and inclusive of all taxes. The cost will also include the training costs also	n) The Price offered by the Bidder to the Bank must be in Indian Rupees and payments will be made to the Bidder in Indian Rupee only. The costs should be ~~inclusive~~ exclusive of duties, insurance, freight, charges of road permit and inclusive of all taxes. The cost will also include the training costs also	No Change in RFP terms.
109	6.13. Terms of Payment and Payment Milestones : Cost of Product including OEM warranty for 3 years	71	p) The payment milestones are defined as below: 50% Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS . 20% Post UAT Sign off (Phase -1) and 30% Post project signoff (Phase-2)	p) The payment milestones are defined as below: ~~50%~~ 90% Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS . ~~20%~~ 5% Post UAT Sign off (Phase -1) and ~~30%~~ 5% Post project signoff (Phase-2)	No Change in RFP terms.
110	6.13. Terms of Payment and Payment Milestones	72	r) Payment for the CSOC monitoring & operations cost, P2P link for DC-DR replication as part of Operational Cost for contract period will be divided into equal quarterly installments and will be payable to the Bidder quarterly in arrears on submission of invoice and other supporting documents.	r) Payment for the CSOC monitoring & operations cost, P2P link for DC-DR replication as part of Operational Cost for contract period will be divided into equal quarterly installments and will be payable to the Bidder quarterly in ~~arrears~~ advance on submission of invoice and other supporting documents.	No Change in RFP terms.
111	6.14. Taxes and Duties	72	The bidder shall be entirely responsible for all applicable taxes, duties, levies, charges, license fees, road permits, etc. in connection with delivery of services at site including incidental services…………………………..f) The price quoted by the bidder should be in Indian Rupee and should be inclusive of all local taxes, VAT, GST, service tax, duties, levies, transportation costs, back to back support with OEM during warranty / AMC, insurance costs, training costs, implementation charges etc., till the bid validity period.	The ~~bidder~~ bank shall be entirely responsible for all applicable taxes, duties, levies, charges, license fees, road permits, etc. in connection with delivery of services at site including incidental services…………………………..f) The price quoted by the bidder should be in Indian Rupee and should be ~~inclusive~~ exclusive of all local taxes, VAT, GST, service tax, duties, levies, transportation costs, back to back support with OEM during warranty / AMC, insurance costs, training costs, implementation charges etc., till the bid validity period.	No Change in RFP terms.
112	6.15. Execution of Agreement and NDA	72	a) The selected bidder should execute agreement with the Bank which will remain valid for at least 3 years extendable upto 5 years at the discretion of the Bank c) The date of Purchase Order shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out with reference to this date	a) The selected bidder should execute agreement with the Bank which will remain valid for at least 3 years extendable upto 5 years at the ~~discretion~~ mutual consent of the Bank and the bidder c) The date of Agreement ~~Purchase Order~~ shall be treated as date of engagement and the time-line for completion of the assignment shall be worked out with reference to this date	No Change in RFP terms.
113	6.16. Period of Contract	73	a) The contract shall commence on the acceptance date of all solutions under CSOC (Phase – 1 Signoff) and continue for a period of THREE years thereafter. The contract may be extended for a maximum period of two years (in total five years) on the same terms and conditions at discretion of the bank. b) The contract can be extended to 4th & 5th year at the discretion of the Bank if required, based on the same terms and conditions. The cost for the fourth and fifth year will be re-negotiated at the end of three year contract period. Bidders are to ensure that all the solutions including hardware, software, services or any other tool supplied will be supported up to 5 years and operations will be carried out for five year	a) The contract shall commence on the acceptance date of all solutions under CSOC (Phase – 1 Signoff) and continue for a period of THREE years thereafter. The contract may be extended for a maximum period of two years (in total five years) on the same terms and conditions at ~~discretion~~ mutual consent of the bank and the bidder. b) The contract can be extended to 4th & 5th year at the ~~discretion~~ mutual consent of the Bidder and the Bank if required, based on the same terms and conditions. The cost for the fourth and fifth year will be re-negotiated at the end of three year contract period. Bidders are to ensure that all the solutions including hardware, software, services or any other tool supplied will be supported up to 5 years and operations will be carried out for five year	No Change in RFP terms.
114	Termination	74	1. d) There has been a breach of confidentiality or there is a cyber-security breach of nature detrimental to the interest of Bank. Decision of Bank in this connection shall be final and binding on the successful bidder.	1. d) There has been a breach of confidentiality or there is a cyber-security breach of nature detrimental to the interest of Bank. ~~Decision of Bank in this connection shall be final and binding on the successful bidder~~.	No Change in RFP terms.

115	Termination	74	2. Termination for insolvency: Bank may at any time terminate the Contract by giving written notice of 30 days to the bidder, if the bidder becomes bankrupt or otherwise insolvent. In this event termination will be without compensation to the bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has occurred or will accrue thereafter to the Bank.	2. Termination for insolvency: Either Party ~~Bank~~ may at any time terminate the Contract by giving written notice of 30 days to the other Party ~~bidder~~, if that other Party ~~the bidder~~ becomes bankrupt or otherwise insolvent. ~~In this event termination will be without compensation to the bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has occurred or will accrue thereafter to the Bank.~~	No Change in RFP terms.
116	Termination	74	3. Terimination for Conveinence: The bank may, at any point during the currency of this contract may terminate the contract by giving 30 days advance notice to the bidders without assigning whatsoever reason. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank	~~The bank~~ Either party may, at any point during the currency of this contract may terminate the contract by giving ~~30~~ ninety (90) days advance notice to the bidders without assigning whatsoever reason. ~~In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank~~	No Change in RFP terms.
117	Termination	74	6.17.2 The Selected bidder shall have right to terminate only in the event of winding up of the Bank.	6.17.2 The Selected bidder shall have right to terminate only in the event of winding up of the Bank and where the Bank has not made payment of undisputed invoices as per payment schedule after receiving a notice regarding the same from the Bidder.	No Change in RFP terms.
118	Termination	75	The Bank shall make such prorated payment for services rendered by the selected bidder and accepted by the Bank at the sole discretion of the Bank in the event of clause of termination, provided that the selected bidder is in compliance with its obligations till such date. However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be applicable to selected Bidder. There shall be no termination compensation payable to the selected bidder.	The Bank shall make such prorated payment for services rendered by the selected bidder and accepted by the Bank ~~at the sole discretion of the Bank~~ in the event of clause of termination, provided that the selected bidder is in compliance with its obligations till such date. ~~However, no payment for “costs incurred, or irrevocably committed to, up to the effective date of such termination” will be applicable to selected Bidder. There shall be no termination compensation payable to the selected bidder.~~ In the event of termination by the bank, the bidder shall be paid for the: a) Goods delivered b) Services rendered c) Work in progress d) Third party orders in pipeline which cannot be cancelled despite Contractor's best efforts e) Unrecovered investments shall be paid by customer as per termination schedule till the date of termination.”	No Change in RFP terms.
119	Right to Visit	77	a) All records of the Bidder with respect to any matters covered by this Tender document/ subsequent order shall be made available to SIDBI or its designees at any time during normal business hours, as often as SIDBI deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.	a) All records (except internal cost records) of the Bidder with respect to any matters covered by this Tender document/ subsequent order shall be made available to SIDBI or its designees at any time during normal business hours, as often as SIDBI deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.	No Change in RFP terms.

120	Indemnity	78	As per RFP	a) The Bidder/ successful bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank by a third party as a result of: i. Bank's authorized / bona fide use of the Deliverables and /or the Services provided by Bidder under this RFP document; and/or ii. ~~An act or omission of the Bidder, employees, agents, sub-contractors in the performance of the obligations of the Bidder under this RFP document; and/or~~ iii. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank; and/or iv. ~~Breach of any of the term of this RFP document and/or of the agreement to be entered subsequent this RFP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty by the successful Bidder under this~~	No Change in RFP terms.
121	Indemnity	79	As per RFP	d) ~~The bidder shall indemnify the Bank and be liable for any loss or damage suffered by the Bank due to malfunctioning of the system as supplied and installed by them.~~ The total liability of the selected bidder shall not exceed the total cost of the order value. e) Indemnity would be limited to limitation of liability ~~court; tribunal or arbitrator awarded damages~~ and shall exclude indirect, consequential and incidental damages. However indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by ~~its customers and/or~~ regulatory authorities.	No Change in RFP terms.
122	Confidentiality	80, 82	As per RFP	Bidder shall suitably defend, indemnify Bank for any loss/damage suffered by ~~Bank~~ any third party on account of and to the extent of any disclosure of the confidential information. k) The confidentiality obligations shall survive the expiry or termination of the agreement between the Bidder and the Bank for a period of 5 years..	No Change in RFP terms.
123	Resolution of Disputes	84	As per RFP	d) Arbitration proceedings shall be held at Mumbai ~~Lucknow~~, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English	No Change in RFP terms.

124	Negligence	86	As per RFP	~~a) 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.~~ ~~b) The below mentioned situations will also be treated as an act of negligence by the Bidder.~~ ~~i. In case of any damage of Bank's property during execution of the work is attributable to the bidder, bidder has to replace the damaged property at his own cost.~~ ~~ii. The selected Bidder shall take all steps to ensure safety of bidder's and the bank's personnel during execution of the contract and also be liable for any consequences due to~~	No Change in RFP terms.
125	Misc	86	As per RFP	Repetative Clause ~~e) Bidder shall indemnify, protect and save SIDBI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting directly or indirectly from an act or omission of Bidder, its employees, its agents, in the performance of the services provided by contract, infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided by Bidder as part of the delivery to fulfill the scope of this project.~~	No Change in RFP terms.
126	Responsibility of Completeness	87	d) The bidder shall supply along with each item all the related documents, Software Licenses and Other Items without any additional cost. The documents shall be in English. These will include but not restricted to User Manual, Operation Manual, Other Software and Drivers etc	Require clarification on the count softwares , user manuals and operational manual required	The bidder is required to provide all trainees with detailed training material and 2 additional copies to the bank for each solution as per the scope of work of the bank.
127	Governing Law and Jurisdiction	88	As per RFP	The RFP and agreement that may be entered into pursuant thereto will be governed by and construed and enforced in accordance with the laws of India and the same shall be subject to the exclusive jurisdiction of the courts in Mumbai ~~Lucknow,~~ India.	No Change in RFP terms.
128	6.46. Business Continuity	92	b) In the event of failure of the bidder to render the service, without prejudice to any other right the Bank shall have as per this agreement, the bank at its sole discretion may make alternate arrangements for getting the services from any other source. And if the bank gives a prior notice to the service provider before availing such service from any other alternative source, the service provider shall be liable to reimburse the expenses, if any incurred by the bank in availing such services from the alternative source.	b) In the event of failure of the bidder to render the service, without prejudice to any other right the Bank shall have as per this agreement, the bank at its sole discretion may make alternate arrangements for getting the services from any other source. And if the bank gives a prior notice to the service provider before availing such service from any other alternative source, the service provider shall be liable to reimburse the expenses, if any incurred by the bank in availing such services from the alternative source upto 10% of the excessive value of teh undelivered hardware or services.	No Change in RFP terms.
129	7. Service Level Agreement & Liquidated Damages	95	c) However the Liquidated damages to be recovered under above clauses shall be restricted & capped to 10% of the total value of the order for each year independently during the contract period.	c) However the Liquidated damages to be recovered under above clauses shall be restricted & capped to ~~10%~~ 3% of the total value of the order for each year independently during the contract period.	No Change in RFP terms.
130	7.2. Liquidated damages for not maintaining uptime	97	n) However, the maximum LD levied shall not be more than the 10% of total value of the order per quarter.	n) However, the maximum LD levied shall not be more than the ~~10%~~ 3% of total value of the order per quarter.	No Change in RFP terms.
131	7.3. SLAs & Liquidity Damages for CSOC Operations	101	As per RFP	Request SIDBI to add " The agreegate SLA penalty / LD for the entire attribute should not exceed 3% of the ACV"	No Change in RFP terms.

132	8. Annexure for Pre-Qualification Criteria	102	Further, we agree to abide by all the terms and conditions as mentioned herein the tender document. We agree to abide by this offer till nine (9) months from the date of last day for submission of offer (Bid).	Further, we agree to abide by all the terms and conditions as mentioned herein the tender document. We agree to abide by this offer till ~~nine (9)~~ one (1) months from the date of last day for submission of offer (Bid).	No Change in RFP terms.
133	Annexure 8.10 Pre-Contract Integrity Pact		3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative to any of the officers of the BUYER or alternatively, if any relative of the officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filling of tender. The term 'relative' for this purpose would be as defined in Section 2 (77) of the Companies Act, 2013. 6 (iv.) To recover all sums already paid by the BUYER, and in case of Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India. If any outstanding payment is due to the bidder from the buyer in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest. 7. Fall Clause The BIDDER undertakes that it has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other	Request customer to delete this clause from the RFP	No Change in RFP terms.
134	10. Annexure for Commercial Bid	136	The Total fee is inclusive of all taxes, duties, charges and levies (as applicable and payable under the local laws) that we might incur and there will be no additional charges whatsoever. We will abide by the payment terms as mentioned in the aforesaid RfP.	The Total fee is ~~inclusive~~ exclusive of all taxes, duties, charges and levies (as applicable and payable under the local laws) that we might incur and there will be ~~no~~ additional charges in case of any change in the tax rates and introdcution of new levies ~~whatsoever~~. ~~We will abide by the payment terms as mentioned in the aforesaid RfP.~~	No Change in RFP terms.
135	Variance in Minimum Wages		Clause not present	Request Addition of the clause " Service Provider undertakes that it is compliant to State minimum wages act at the time of execution of the Agreement and the commercials are accordingly factored. In the event there is a change to the State minimum wages act or if the Customer wants the Service Provider to comply to some other minimum wages act including but not limited to Central minimum wages act or the existing minimum wages act is repealed by another act, then in such cases, Customer will support Service provider with change request for additional cost incurred by Service Provider for complying to new minimum wages. Service provider will not ask for Change request for any changes that is within 8% increase year on year from the State minimum wages as on the date of contract sign off."	No Change in RFP terms.
136	Pass Through Warramty		Clause not present	Request Addition of the clause "Since bidder is acting as a reseller of completed products, bidder shall "pass-through" any and all warranties and indemnities received from the manufacturer or licensor of the products and, to the extent, granted by such manufacturer or licensor, the Customer shall be the beneficiary of such manufacturer's or licensor's warranties and indemnities. Further, it is clarified that Bidder shall not provide any additional warranties and indemnities with respect such products."	No Change in RFP terms.
137	Risk and Title		Clause not present in RFP	Request Addition of the clause "The risk, title and ownership of the products shall be transferred to the customer upon delivery of such products to the customer"	No Change in RFP terms.

138	Saving Clause		Clause not present in RFP	Request Addition of the clause " Bidder's failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Bidder performance is effected , delayed or causes non-performance due to Customer's omissions or actions whatsoever. "	No Change in RFP terms.
139	Deemed Acceptance		Clause not present in RFP	Request Addition of the clause "Services and/or deliverables shall be deemed to be fully and finally accepted by Customer in the event when Customer has not submitted its acceptance or rejection response in writing to Bidder within 15 days from the date of installation / commissioning or when Customer uses the Deliverable in its business, whichever occurs earlier. Parties agree that Bidder shall have 15 days time to correct in case of any rejection by Customer."	No Change in RFP terms.
140	Change Order		Clause not present in RFP	Request Addition of the clause "Either party may request a change order ("Change Order") in the event of actual or anticipated change(s) to the agreed scope, Services, Deliverables, schedule, or any other aspect of the Statement of Work/Purchase Order. Bidder will prepare a Change Order reflecting the proposed changes, including the impact on the Deliverables, schedule, and fee. In the absence of a signed Change Order, Bidder shall not be bound to perform any additional services. "	Already covered, please refer to Section 6.11 of the RFP
141	4.1. Security Information and Event Management	39	A. Solution Implementation k) The bidder should provide SIEM license for 10000 EPS from day 1	As per Annexure 11.1, Initial EPS requirement is for 5000. But in this clause bank has asked for SIEM License for 10000 from day 1.Request bank to confirm the EPS count for which we need to quote.	The bidder has to provide SIEM license for 10000 license and storage for minimum 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
142	4. Scope of Work	39	j) The logs collected by the SIEM log collector should be replicated across primary Data Center and Disaster Recovery location. The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder.	As we do not have Telecom Service provider license, we can't sell/resell the bandwidth. Request bank to delete this clause.	The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder. If required, SIDBI will enter into a tri-party agreement with the bidder and service provider for obtaining P2P link. The uptime of this link will be the responsibility of the service provider providing P2P link.
143	4. Scope of Work	47	4.8.1 g) There should be three separate environments: Development, Test (UAT), and Production (DC-DR). The environments must be configured on a separate physical servers. The Development environment should have at least 20% and Test (UAT) environments should have at least 50% of the configuration of the Production environment quoted by the Bidder.	The solutions asked in RFP are for monitoring & alert/Incident tracking from the perspective of security. There will not be any application/product development for the solutions asked. Hence request bank to remove Development & Test (UAT) environment.	No Change in RFP terms.
144	5. Evaluation Methodology	61	5.1 C. Scoring for Client Feedback (TF) a) The Bidders are requested to fill detailed information on past implementations / engagements for all the solutions as per below format.	Request bank to confirm for what does "all the solutions" means and confirm if we can give feedback for more than 2 customers. Also confirm if this should be in line pre-qualification criteria mentioned in Annexure 8.2 Point no 6 & point no 7.	All the solutions refer to solutions mentioned here as part of this RFP. The minimum requirement is for two customers as part of scoring for client feedback and evaluation will be done only for two customers.

145	5. Evaluation Methodology	61	5.1 D. Scoring for Resources having required Certification (TC) a) The bidder is required to provide certifications of employees on permanent payroll having ISO 27001 LI/LA or CISA or CISSP or CISM.	In this RFP, Bank has asked to supply & implement SIEM,PIM,Anti-APT,Firewall Ananlyer & NAC. We request bank to consider the resources with certification for these solution. Apart from these solutions, Bank has also asked for VAPT & Threat intelligence services. Keeping in view of these services, we request bank to also consider resources with CEH & CRISC. Hence request bank to consider following clause: The bidder is required to provide certifications of employees on permanent payroll having ISO 27001 LI/LA or CISA or CISSP or CISM or CEH or CRISC or certified resources of qualified SIEM platform.	No Change in RFP terms.
146	4.10. Implementation Phases and Timelines	56	b) Phase 2 – Integration of Bank's remaining in-scope devices with SIEM and other security tools. The project signoff for SIEM, PIM and NAC will be given post integration of 95% of total devices/users mentioned in Annexure 11.7. However, the bidder is responsible for integration of all devices/users.	Request bank to provide timeline for project sign off	The project signoff for SIEM, PIM and NAC will be given post integration of 95% of total devices/users mentioned in Annexure 11.7.
147	4.8.6. Monitoring	54	The CSOC operations and monitoring will be carried out from Chennai location during the contract period. However, bidder needs to deploy one dedicated resource at DC site, Navi Mumbai.	Request bank to provide seating arrangement for resources deployed at DC & DR.	The bank will provide seating arrangement for CSOC operations at Chennai and at DC Site, Navi Mumbai.
148	Bid Validity/ बोली के वैधता	3	Nine Month from the last date of bid submission	OEM doesn’t give price validity of more than 3 months. Request bank to change this to 3 months.	No Change in RFP terms.
149	3.2. Objective	23	The Bank has plans to co-locate the DR Site from third party Data Center at Chennai and the order has already been issued for the same. The bidder should continue provide security services for co-located DR setup in future.	Our understanding is the IP schema will remain the same, only physical location will be different. Please clarify.	The interpretation is correct.
150	4.5. Network Access Control (NAC),i)	44	The Bank has offices at around 80 locations in addition to the DC and DR. Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, Bank has placed order for implementation of SD-WAN based IP MPLS network. The routers at the locations will be replaced with SD-WAN CPEs. The proposed solution should be able to capture logs from the CPE’s installed at the locations. The Bidder’s proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period.	Request bank to share the OEM of SDWAN CPEs in order to check the compatibility with NAC.	The hardware / software / devices / appliances are from the leading manufactures. The details will be shared with successful bidders.
151	4.8. Other General Requirement,4.8.1. Hardware, Software and Network Connectivity,	46	e) The bidder needs to propose only Veritas backup solution for backups.	Request bank to allow bidder to quote backup solution from other OEM as well. This is limiting the competition.	No Change in RFP terms.
152	4.8. Other General Requirement,4.8.1. Hardware, Software and Network Connectivity,	47	h) Bidder should consider sizing as part of integration of additional devices during the contract period. SIDBI will not be responsible to pay for any additional cost other than the cost mentioned in commercial bid.	Request bank to provide incremental value or percentage of additional devices bank foresee to add in near future in their environment. This will help in our solution sizing.	Refer to Annexure 11.7 of the RFP.
153	4.8.2. Training	47	c) The bidder and OEM are required to provide training jointly as per the below table for people nominated by the bank for each solution specified in the scope of work. d) The bidder and OEM are required to provide ad-hoc trainings to the bank staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. Bank has the right to exercise this training option at its discretion. The cost of this training would need to be quoted in the Commercial Bid by the bidder in the pre-defined field.	Bidder has expertise in the solution which bank has asked.Hence we request to consider following: c) The bidder/OEM/ OEM Nominated training partener are required to provide training jointly as per the below table for people nominated by the bank for each solution specified in the scope of work. d)Only The bidder is required to acquaint bank with the latest features and functionalities of the solutions for minimum of one day.	No Change in RFP terms.

154	4.8.2. Training	47	c) The bidder and OEM are required to provide training jointly as per the below table for people nominated by the bank for each solution specified in the scope of work. d) The bidder and OEM are required to provide ad-hoc trainings to the bank staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. Bank has the right to exercise this training option at its discretion. The cost of this training would need to be quoted in the Commercial Bid by the bidder in the pre-defined field.	Request bank to confirm where to add ad-hoc training cost in commercial bid format.	The bidder needs to consider this as part of the post implementation training field in commercial bid.
155	4.8.3. Implementation & Integration	49	p) Any interfaces required with existing applications/ infrastructure within the bank should be developed by the bidder for successful implementation of the CSOC as per the defined scope of bank.	Request bank to confirm if bank is looking for any API integration or customization. If yes please share details.	The integration is not limited to API integration.
156	4.8.3. Implementation & Integration	49	r) In case the CSOC on-going operations are part of scope for a particular bank, 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 bank.	This will be limited to EPS sizing mentioned in the RFP. Any additional requirement will be on purchase additional license. If bank has details of this additional requirment, request to share the same	No Change in RFP terms.
157	4.8.3. Implementation & Integration	50	z) OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM,through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.	Bidder has expertise in the solution which bank has asked. Hence we request to consider following: Initial installation, configuration and integration should be done by the Bidder/OEM.	The Bidder would be the single point of contact. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.
158	4.8.3. Implementation & Integration	51	hh) CSOC set up should assure the compliance to the Indian regulatory requirements, ISO27001 standards and also international regulations and laws where bank has its presence. The bidder is expected to study the regulations and comply with them as and when mandated.	We will comply with new regulation and guidelines. However if there are any commercial impact or additional purchase requirement, Bank need to bear the cost of the same.	No Change in RFP terms.
159	4.8.7. Continuous Improvement	55	d) Bidder needs to update all solutions and Cyber Security Operations Centre (CSOC) based on any new regulations and RBI guidelines	We will comply with new regulation and guidelines. However if there are any commercial impact or additional purchase requirement, Bank need to bear the cost of the same.	No Change in RFP terms.
160	6.13. Terms of Payment and Payment Milestones	72	r) Payment for the CSOC monitoring & operations cost, P2P link for DC-DR replication as part of Operational Cost for contract period will be divided into equal quarterly installments and will be payable to the Bidder quarterly in arrears on submission of invoice and other supporting documents.	Request bank to pay this in quarterly in advance	No Change in RFP terms.
161	9. Annexure for Technical Bid	131	2. The EOL / EOS of each solution should cover the CSOC project timeline of the Bank. If End of Life (EoL) or End of support (EoS) date announced by the OEM, the bidder will be responsible for replacing / upgrading the solution. In case such date is not announced, it should be supported for minimum five years.	Bidder is responsible for replacing the product if it has reach End of Support only.	No Change in RFP terms.
162	6.13. Terms of Payment and Payment Milestones	70	The payments for services will be released on quarterly basis as arrears for all the implemented solutions and services.	Request Bank to release payment for services on yearly advance basis	No Change in RFP terms.
163	6.13. Terms of Payment and Payment Milestones	71	Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost) 50% - Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS 20%- Post UAT signoff (Phase-1) 30% - Post project signoff (Phase-2)	Request Bank to consider: Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost) 80% - Delivery of SIEM,CSOC Solution License, Hardware and Storage , Other Software License, after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS 10%- Post UAT signoff (Phase-1) 10% - Post project signoff (Phase-2)	No Change in RFP terms.

164	6.13. Terms of Payment and Payment Milestones	71	Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost) 50% - Delivery and acceptance of the SIEM and CSOC solution License with Environment Setup after post-delivery verification, on submission of invoice with Proof of Delivery, Proof of Entitlement, Proof of Warranty / AMC / ATS 20%- Post UAT signoff (Phase-1) 30% - Post project signoff (Phase-2)	Request bank to release the payment solution wise for all stages.	No Change in RFP terms.
165	7.1. Liquidated damages for delay in Delivery and Installation of Hardware and Software	95	b) In case, if there is delay in delivery of the hardware & software, installation of the security solutions and associated hardware, software and software licenses, as given in commercial bid, beyond the schedule given in Section 4.10 from date of issue of PO, then LD at the rate of 1% per week of the cost quoted against each of respective item as mentioned in Commercial Bid for items not delivered will be levied per week or part thereof (on pro rata basis for the no. of days) and deducted against bills submitted.	Request Bank to Consider: b) In case, if there is delay in delivery of the hardware & software, installation of the security solutions and associated hardware, software and software licenses, as given in commercial bid, beyond the schedule given in Section 4.10 from date of issue of PO, then LD at the rate of 0.5% per week of the cost quoted against each of respective item as mentioned in Commercial Bid for items not delivered will be levied per week or part thereof (on pro rata basis for the no. of days) and deducted against bills submitted.	No Change in RFP terms.
166	7.1. Liquidated damages for delay in Delivery and Installation of Hardware and Software	95	c) The integration of all the security solutions with SIEM should be completed within a period as mentioned in the section 4.10 from the date of issue of PO. In case of delay in integration beyond three months, LD at the rate of 1% per month of the cost quoted against SIEM as mentioned in Commercial Bid will be levied per month for the no of days of delay (on pro rata basis for the no. of days) and deducted against bills submitted.	Request Bank to Consider: c) The integration of all the security solutions with SIEM should be completed within a period as mentioned in the section 4.10 from the date of issue of PO. In case of delay in integration beyond three months, LD at the rate of 0.5% per month of the cost quoted against SIEM as mentioned in Commercial Bid will be levied per month for the no of days of delay (on pro rata basis for the no. of days) and deducted against bills submitted.	No Change in RFP terms.
167	7.1. Liquidated damages for delay in Delivery and Installation of Hardware and Software	95	CSOC Operations Failure including any device (hardware / software) failure resulting in failure of CSOC operations	Request Bank to Consider: 99% and above NA 97% to 99% - 0.5% of Total CSOC Monitoring and Operations cost for each failure 95% to 96.99% - 2% of Total CSOC Monitoring and Operations cost for each failure	No Change in RFP terms.
168	7.2. Liquidated damages for not maintaining uptime	96	Individual Security /Device solution (Hardware / Software) Failure (including Incident Management Tool, SAN, backup tape solution). SIEM failure will be considered as total failure and liquidated damage will be as per the point 1.	Request bank to consider: 99% and above - NA 97% to 99% - 1% of Notional AMC charges for each failure 95% to 96.99% - 5% of Notional AMC charges for each failure Less than 95% - 10% of Notional AMC charges for each failure	No Change in RFP terms.
169	7.2. Liquidated damages for not maintaining uptime	97	l) For the L1, L2 and L3 resources for the leave of absence: - Each on-site resource shall be granted a maximum up to 01 (One) day leave per month. However, substitute should be provided. LD will be levied for any absence for which no substitute is arranged by the Service Provider as per defined in the below table. The LD charges will be in addition to the pro rata charges for the resources for their days of absence	Request Bank to consider: • L1 Resource - Rs.500/- per day maximum Rs.10000/- per month • L2 Resource - Rs.1000/- per day maximum Rs.10000/- per month • L3 Resource - Rs 1000/- per day maximum Rs 10000/- per month	No Change in RFP terms.
170	Annexure 11.4 Firewall Analyzer	163, Point number 10	The proposed solution should allow opening a Change Request for removing the Unused Rules and Covered rules directly from the analysis report for ease of operations. The removal of these rules should also be automatic irrespective of the firewall brand in case bank decides to procure change management module as well from the same OEM in near future.	Please confirm if SIDBI would like to procure the Firewall Change Management solution and whether that should be available from the day one during the Implementation?	The proposed solution should have mentioned capability.
171	Annexure 11.4 Firewall Analyzer	163, Point number 11	The proposed solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices	Please confirm total number of L3 Routers/Switches to build the network map automatically? Pls confirm total number of Physical and Virtual Firewall clusters/Pair?	Refer Annexure 11.7. The details will be shared with successful bidder.
172	Annexure 11.4 Firewall Analyzer	164, Point number 14	The proposed solution should have a change management capability and should support Bulk change request submission through Excel file	Please confirm if SIDBI needs Firewall change management capability also from the day one?	The proposed solution should have mentioned capability.

173	Annexure 11.4 Firewall Analyzer	165, Point number 26	The Proposed solution should have a scalability factor to discover and map the business applications and the associated logical connectivity with the underlying security policies. It should also be able to build the application flows based on the Firewall policies if required.	Please confirm what does scalability means? Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should be scalable and have mentioned capability if the bank requires in future.
174	Annexure 11.4 Firewall Analyzer	165, Point number 27	Solution should identify Blocked and allowed flows from an application perspective to enable application team to collaborate with the operations team	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
175	Annexure 11.4 Firewall Analyzer	165, Point number 29	The proposed solution should have a provision of decommissioning of business application. The decommissioning process should be fully automated and the rules should be removed automatically from the Firewalls only for that application which needs to be decommissioned. The system should also identify those rules which cannot be removed as those could be linked to other applications.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
176	Annexure 11.4 Firewall Analyzer	165, Point number 30	The proposed solution should be application centric and have a provision for server migration process. The process should be fully automated and should specify the inline applications and their logical connectivity which requires changes. The proposed system should even provision the necessary rules on the FW's automatically.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm the number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
177	Annexure 11.4 Firewall Analyzer	165, Point number 31	The solution should provide an ability to verify the impact on business applications if the inline FW is down or a specific policy on the FW is blocking the application traffic	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
178	Annexure 11.4 Firewall Analyzer	165, Point number 32	The proposed solution should have a capability to map the Firewall configuration risks with the inline business applications. It should present the risks in the overall application context	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
179	Annexure 11.4 Firewall Analyzer	Page 33, Point A	Data Centre and DR Site	Please confirm if the solution is required in HA-DR architecture or only at DC as a standalone solution?	Please refer Section 4 Scope of Work of RFP.
180	Annexure 11.5 Network Access Control (NAC)	166	The solution should be able to link and identify iPads that are owned by the Bank, and block other iPads	Request you to change point as follows "The solution should be able to link identify iPads that are owned by the Bank, and block other iPads by integrating with MDM Solutions". Ths is funcionality of MDM. It can be achieved by the MDM solution	The solution should be able to allow access of iPads that are owned by the Bank, and block other iPads by integrating with MDM Solutions
181	Annexure 11.5 Network Access Control (NAC)	167	The solution should support alerting mechanism such as e-mail, SMS etc.	Request to modify as- The solution should support alerting mechanism such as e-mail, SMS etc by integrating with the Sylog and SIEM solutions. We can pass the logs to an existing Syslog or a centralized NMS server. These servers can trigger such alerts not only for the NAC solution but as a centralized alerting mechanism for all network and security infrastructure elements	No Change in RFP terms.
182	Annexure 11.5 Network Access Control (NAC)	167	The solution should permit admin to define thresholds for threat levels received from the NAC	Request you to remove point because this is not NAC functionality. NAC mainly focus over network authentication, authorization and endpoint assesment. Threats can be mangement by endpoint protection, firewall and IPS solutions. Pulse NAC can integrate with them directly or through REST API.	No Change in RFP terms.
183	Annexure 11.5 Network Access Control (NAC)	167	The proposed solution should provide scanning to discover and mitigate threats from infected endpoints and incorporate the indicators of compromise (IOC's) the bank receives from time to time from external sources.	Request to remove point. IOC & vunerbility scanning and threat mangement is something not relevent to NAC. So need to remove this. However our NAC solutions support adaptive security approach to restrict suspected users based on behaviour analysis and Artificial intelegence.	No Change in RFP terms.

184	VAPT service		Addition	Solution shall allow API integration with other systems or be able to automate workflow. The API can be used by pentesting tool for authentication purpose, for creating tasks in automating pentesting, etc	No Change in RFP terms.
185	VAPT service		Addition	The proposed solution must be able to support for centralized management of distributed scanners. Solution must be able to scan multiple network segments. No licensing cost should be imposed due to need for reporting task, user access, configuration, administration, and additional distributed on-premise scanners. This will help Sidbi to use all the features and functioning of the solution wihtout any issues/limitation related licenses.	No Change in RFP terms.
186	VAPT service		Addition	The proposed solution must support for consolidated reporting in large deployments without any additional add-ons or fees required. This will help Sidbi to use all the features and functioning of the solution wihtout any issues/limitation related licenses.	No Change in RFP terms.
187	VAPT service			The proposed vulnerability management solution must be able to offer an API capability. Describe how the API is accessed, and what functions are available. Are there any additional modules or fees associated with the API? Describe what data elements/features in your portal are not accessible via your API.	No Change in RFP terms.
188	VAPT service			The proposed Vulnerability management solution must support the automatic discovery of virtual assets on: - Vmware vCenter - Vmware ESX/ESXi and Support hypervisor scanning of virtual assets on - Vmware NSX	No Change in RFP terms.
189	VAPT service			The proposed vulnerabilit y management solution must provide a correlated list of: - exploit modules available for each vulnerability - malware kits available for each vulnerability - automatic workflow to validate vulnerability in the proposed pentesting tool. If pentesting tool can seamlessly import the vulnerability from VM tool and validate it and share back the validated vulnerabilites information to VM tool then it will be easier for Sidbi team to decide and priortise the remediation plan against the listed vulnerabilities.	No Change in RFP terms.
190	11.7 Indicative List of hardware / network / security devices	170	Number of devices to be integrated with PIM	Request bank to please mention the number of privileged users to be integrated with the PIM/PAM solution	Refer to Annexure 11.7 of the RFP. The number of devices to be integrated with PIM is 200. The number of privileged users to be integrated with PIM solution are 70.
191	Annexure 11.1 Security Information and Event Management ⍰	143, Requirement Description	The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope	As per our understanding "Propose solution should be appliance based and separate hardware for collection, loging and correlation". Is our understanding correct?	The interpretation appears to be correct. The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module.
192	Annexure 11.1 Security Information and Event Management ⍰	143, Requirement Description	Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	As per our understanding "Propose hardware should be capable to handle sustained 20,000 EPS along with storage from Day 1". Is our understanding correct?	The bidder has to provide SIEM license for 10000 license and storage for minimum 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.

193	Annexure 11.1 Security Information and Event Management ⍰	144, Log taxonomy & Categorization	The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis.	Please share Network Throughput to size Packet Capture solution. Ex: " Packet capture solution should support 1 Gbps traffic along with 4 network ports (2 X 1 Gbps + 2 X 10 Gbps)	The bank currently has network throughput of 10 Gbps traffic.
194	Annexure 11.1 Security Information and Event Management ⍰	147, Dashboard & Reporting	The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities	As per our understanding this point relate to investigate the incidents. Need clarity on report as report can be generate as per pending incidents and analyse can be done on pending mitigation activities. IS our understanding correct	The interpretation appears to be correct. The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities
195	Annexure 11.1 Security Information and Event Management ⍰	149, Storage	System should have capacity to maintain the logs for 90 days on Tier I storage and older logs should be archived on Tier II storage and Tier 3 storage	As per our understanding storage should be sized for 20,000 EPS from Day 1. Is our understanding correct?	The bidder has to provide SIEM license for 10000 EPS and storage for minimum 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
196	Annexure 11.1 Security Information and Event Management ⍰	29, Log taxonomy & Categorization	The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis.	This point requires Packet analysis/DPI solution, please suggest if the same is required, as the RFP mentions that scope is for log collection & correlation only, In case if Packet analysis/DPI solution is required, please provide the no of interfaces per location & flow bandwidth per location details for solution sizing along with data retention Policy	The proposed solution should have mentioned capability.
197	Annexure 11.1 Security Information and Event Management ⍰	54, Event Filtering & Analysis	The proposed Solution should be able to filter the captured packets based on layer-2 to layer-7 header information. The solution should also provide ability to reconstruct data payload.	This point requires Packet analysis/DPI solution, please suggest if the same is required, as the RFP mentions that scope is for log collection & correlation only, In case if Packet analysis/DPI solution is required, please provide the no of interfaces per location & flow bandwidth per location details for solution sizing along with data retention Policy	The proposed solution should have mentioned capability.
198	Annexure 11.1 Security Information and Event Management ⍰	55, Event Filtering & Analysis	The solution must have the ability to capture network traffic and import PCAP files.	This point requires Packet analysis/DPI solution, please suggest if the same is required, as the RFP mentions that scope is for log collection & correlation only, In case if Packet analysis/DPI solution is required, please provide the no of interfaces per location & flow bandwidth per location details for solution sizing along with data retention Policy	The proposed solution should have mentioned capability.
199	Annexure 11.1 Security Information and Event Management ⍰	63, Dashboard & Reporting	The dashboard should show the status of all the tools deployed as part of the SOC, including availability, bandwidth consumed, system resources consumed (including database usage)	SIEM solution can present the data in dashboard, provided such parameters are forwarded by log sources, please confirm if the solutions deployed can forward such data/logs to SIEM solution.	Availability, threshold and consumption are part of health monitoring. No change in RFP clause.
200	Annexure 11.1 Security Information and Event Management ⍰	76, Dashboard & Reporting	Should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM	Solution can create Email notification, & for SMS notifications, SMS gateways has the feature to receive input as Email & convert it into SMS which can be sent as notification, please confirm if that suffice the requirement.	No change in RFP terms.
201	Annexure 11.1 Security Information and Event Management ⍰	93, Availability	The 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.	Solution supports HA, please suggest if HA is required at all levels/layers i.e. Collection, Processing & Console or only at Collection layer	Please refer Section 4 Scope of Work of RFP.
202	Annexure 11.1 Security Information and Event Management ⍰	113, Integration	Should be able to integrate with bank's existing backup solution for performing backup of the SIEM.	Please provide details of existing backup solution.	Please refer Section 4 Scope of Work of RFP.
203	4.8.3. Implementation & Integration	48	A comprehensive strategy should be provided by the Bidder on implementing the end to end CSOC solution within 7 days of issuance of Purchase Order (PO).	Request you to provide atleast 15 days to provide comprehensive strategy as there are multiple solutions.	No Change in RFP terms
204	4.10. Implementation Phases and Timelines	56	a. Submission of Detailed Project Plan b. Placing of order with OEMs for supply of hardware, software security tools/solutions c. Placing of order for connectivity link (if any)	Request bank to provide 4 weeks from acceptance of PO	Refer to Corrigendum - 2
205	4.10. Implementation Phases and Timelines	56	a. Preparation for CSOC setup and implementation of required processes.	Request bank to provide 5 weeks from acceptance of PO	Refer to Corrigendum - 2

206	4.8.2. Training	47	The bidder and OEM are required to provide ad-hoc trainings to the bank staff, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. Bank has the right to exercise this training option at its discretion. The cost of this training would need to be quoted in the Commercial Bid by the bidder in the pre-defined field.	Request bank to provide the number of Ad hoc training to be conducted yearly	Please refer section 4.8.2 Training of RFP.
207	4.10. Implementation Phases and Timelines	57	Delivery of CSOC Hardware / Software and licenses and resources	Request bank to consider 10-12 weeks from acceptance of PO	Refer to Corrigendum - 2
208	4.10. Implementation Phases and Timelines	57	Deployment of CSOC Resources at Bank's premises	Request bank to consider 12 weeks from acceptance of PO, after interview of candidate	Refer to Corrigendum - 2
209	4.10. Implementation Phases and Timelines	57	Installation & Configuration of SIEM and other Security Tools / Solutions	Request bank to consider 12 weeks from arrival of material	Refer to Corrigendum - 2
210	4.10. Implementation Phases and Timelines	57	Integration of SIEM with other Security Tools / Solutions under CSOC	Request bank to consider 15 weeks from arrival of material	Refer to Corrigendum - 2
211	4.10. Implementation Phases and Timelines	57	User Acceptance Test (UAT) and making the CSOC operational	Request bank to consider 20 weeks from arrival of material	Refer to Corrigendum - 2
212			Additional Queries	Entire project execution & planning will happen through Mumbai	The CSOC operations will be carried out from Chennai. However one resource is required at Mumbai DC site.
213	Annexure 11.1 Security Information and Event Management	143	The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope.	Suggestion: This being a reletively small EPS requirement we would suggest using either a virtual server or provide appliance using locally procured hardware. We understand that all logs are generated within the datacentre iselft and if the design allows can we propose to use a single box deployed in HA mode to be allowed.	No change in RFP terms.
214	Annexure 11.1 Security Information and Event Management	143	Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	Clarification: It should be scalable to 10,000 or 20,000 EPS. With 10,000 EPS we could propose a single box solution while for 20,000 EPS we would need to propose 2 boxes .. Please clarify what is the expectation - to use the same hardware that we propose to be able to withstand 10,000 EPS or 20,000 EPS	The bidder has to provide SIEM license for 10000 EPS and storage for minimum 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
215	Annexure 11.1 Security Information and Event Management	147	Should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM	Please provide SMS gateway details - solution can send emails to SMS gateway in the form of email which can then be transfored into SMS by the gateway	The details will be shared with the selected bidders.
216	Annexure 11.1 Security Information and Event Management	93	The 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.	Only collector HA is metioned - do we need to prpose HA at Dashboard and correlation layers as well.	The solution should support high availability feature. Please refer section 4 Scope of Work of RFP.
217	7.3. SLAs & Liquidity Damages for CSOC Operations	98, Monitoring, Analysis & Incident Reporting	Service Level, 1) Critical events within 15 minutes of the event identification. 2) High priority events within 30 minutes of the event identification. 3) Medium and Low priority events within 60 minutes of the event identification.	Request bank to consider the following 1) Critical events within 1 hour minutes of the event identification. 2) High priority events within 2 Hours of the event identification. 3) No SLA on Medium and Low priority events	No change in RFP terms.
218	7.3. SLAs & Liquidity Damages for CSOC Operations	99	Incident Resolution	Request bank to consider following point, there is no SLA on incident resolution we will onky cooperate uring incident resolution , plz remove SLA as we don have control banks infra & devices	The closure of the incident lies with the bidder however Bank will provide necessary support during the closure.
219	7.3. SLAs & Liquidity Damages for CSOC Operations	100	VAPT advisory & remediation services, point 4, 4. Delay in implementing the resolution in banks test setup for more than 5 days after getting approval from bank will incur Rs. 500 per instance.	this is on the bank & service provider, request you to remove this point.	No change in RFP terms.
220	7.3. SLAs & Liquidity Damages for CSOC Operations	99	Vulnerability Assessment	No SLA is accepted on VA Scan we will only exceute the task	No change in RFP terms.
221	7.3. SLAs & Liquidity Damages for CSOC Operations	101	Security Intelligence Services	Please remove this point as this is service dependent	No change in RFP terms.

222	7.3. SLAs & Liquidity Damages for CSOC Operations	101	New Patches, A delay of more than Five days will incur a LD of 10% of quarterly CSOC Monitoring and Operations cost for that quarter.	Request bank to consider 10% amc cost For that particluar solution for the quarter	No change in RFP terms.
223	7.3. SLAs & Liquidity Damages for CSOC Operations	101	Security Device Management and Administration	This is not pratically fesible request the bank to modify or deleted it	No change in RFP terms.
224	7.3. SLAs & Liquidity Damages for CSOC Operations	101	Optional Components	Request bank to remov this	No change in RFP terms.
225	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have breach detection rate of more than 99% as per NSS lab Breach Detection Systems test report & the test report should be submitted	Considering latest cyber security trends & breaches, Requesting bank to emphasis on Breach Prevention rather than detection only. Requesting Bank to consider NSS BPS Breach Prevention system test report with Block rate of 99% & above as per latest NSS BPS Report.	No change in RFP terms.
226	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects without relying upon any external box solution like Firewall / NGFW / IPS/NGIPS/Web Proxy.	Threats/IOC detected by Anti-APT & relevent intelligence should be shared across all security solutions including NGFW/NIPS for end-to-end protections at their level. Requesting bank revise clause to build shared intelligence architecture by integrating Anti-APT with NGFW.	No change in RFP terms.
227	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed Solution should have throughput of 2 GBPS, have the ability to support both inline and out-of-band detection and should cause limited interruption to the current network environment. The Bank reserves the option of using deployment as Inline or out-of-band.	Anti-APT solution performance is also depend on no. of files emulated per hour/day/month as undersize appliance can add latency in network. Need additional appliance sizing information such as no. of emails/internet users & total no. of emails with attachment received per day/month, similarly total no. of files download happens through proxy per day/month. This data will help to size right appliance considering the user & file emulation capacity of device.	The average number of mails sent and received for one month: Sent - 12,000 Received - 60,000.
228	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack and the history of the movement of the malware in the network.	Kindly confirm if bank is also looking for Endpoint EDR agent solution for worksstations as part of this RFP. If Yes kindly share total no. of endpoints as well as OS flavours to consider.	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
229	Annexure 11.3 Anti – Advanced Persistent Threat / Performance	159	Solution should have a provision of 10G interfaces on Appliance proposed for Data ports.	Kindly confirm the no. of 10 GE interfaces to be considered ??	10G interface is not required currently. However the proposed solution should have provision of 10G interfaces on Appliance proposed for Data ports.
230	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed solution should have capability of horizontal scalability.	Bank should consider Anti-APT in HA pair per site DC/DR which will protect bank network & traffic will not be allowed without inspection even in case of device failure.	No change in RFP terms.
231	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed Solution should be address HTTP,HTTPS,SMTP,SMTP CIFS, FTP and other protocols	Requesting bank to add on-box SSL inspection support to prevent threats coming through SSL or polymorphic channel. Requesting Bank to add specification as "Proposd Soluton should support on-box SSL inspection feature to prevent attack originating from SSL & Polymorphic Channel."	No change in RFP terms.
232	Annexure 11.3 Anti – Advanced Persistent Threat/Endpoint Detection and Response	160	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp	Requesting bank to delete support for .chm & .com file-type as it's avoiding renowed vendor to participate. Kindly confirm if it is acceptable to be added as future enhancement.	No change in RFP terms.

233	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Bank has asked for Multi-layer security methodolgy which includes Anti-Virus & Anti-bot along with Sandboxing. MAC & linux based malwares can be detected through windows platform based APT using multi-inspect engine & threat intel from cloud. Requesting bank to allow only Windows platforms & not both which disallows renowed vendor from RFP participation.	No change in RFP terms.
234	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Mobile malware come as .apk file & requires mobile specific ennviornment to emulate it. Kindly confirm if Bank is looking for separate Mobile solution as part of Mobile Security in this RFP ? If Yes, Kindly share the total no. of Mobile devices to be considered ??	There is no separate requirement for mobile security solution. However, the solution should support monitoring of mobile malwares for the connection originating from the mobile devices.
235	Annexure 11.3 Anti – Advanced Persistent Threat	161	The proposed solution should Block and hold file from spreading across all endpoints i.e. prevent lateral movement	We recommend bank to consider Endpoint EDR agent solution as part of this RFP which will protect lateral movements irrespective of Endpoint location such as online or offline (Roaming Laptops)	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
236	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	161	The solution should support CLI, and must be administered through a web based console using SSH/HTTPS. Should support AAA for role based administration	Considering the huge CVE list of Browser exploits & vulnerabilities getting discovered every year. Requesting Bank to consider agent based console as more secure & fastest configuration mode. Requesting to add software console based configuration mode as well. Requesting Bank to revised clause as "The solution should support CLI, and must be administered through a web based/agent based console using SSH/HTTPS. Should support AAA for role based administration	No change in RFP terms.
237	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	158	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects without relying upon any external box solution like Firewall / NGFW / IPS / NGIPS / Web Proxy	This clause will restrict many sandboxing OEM to bid for RFP who are even offering better security than sandboxing vendors. So requesting to remove this clause.	No change in RFP terms.
238	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	160	The proposed solution should have an automated Incident analysis function that provides a comprehensive view of attack flow, root cause, business impact, and entry point to enable accelerated remediation	It is very difficult to provide business impact so requesting to remove the same.	No change in RFP terms.
239	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	161	The proposed solution should Block and hold file from spreading across all endpoints i.e. prevent lateral movement	This requires endpoint agent. Pls share how many endpoints we need to factor in our solution.	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
240	Section 5.2.D - Scoring for Resources having required Certification (TC)	61	The bidder is required to provide certifications of employees on permanent payroll having ISO 27001 LI/LA or CISA or CISSP or CISM.	Request SIDBI to accept resources who are certified for CEH as well	No change in RFP terms.
241	Section 5.2.D - Scoring for Resources having required Certification (TC)	61	The bidder will be awarded a maximum of 15 marks as per the following:	Request SIDBI to change the marking criteria as below: Minimum of 5 employees - 5 Marks More than 5 and less than or equal to 10 - 10 Marks More than 10 employees - 15 Marks	No change in RFP terms.
242	5.3 Commercial Evaluation of the Bidders	62	The bidder with lowest Total Cost will be declared as L1 and successful bidder, subject to corrections in arithmetic errors	We request SIDBI to make the evaluation on QCBS basis by giving a techno commercial ratio of 70:30	No change in RFP terms.
243	Bid Validity	3	Nine Month from the last date of bid submission	Nine months is very long period for bid validity as the prices are dependant on exchange rate fluctuations. Kindly request the bank to reduce the bid validity to 4 months.	No change in RFP terms.
244	Important Clarifications	4	g) “The Project Site” means Mumbai Office, Chennai Office and Bank’s Data Centers at Navi Mumbai and Chennai. The project team shall operate from Chennai Office and/or Mumbai Office. However, final decision on place of operation will be taken by the Bank as per requirement.	We would request the bank to notify the bidders about the location before submission of the proposal so that relevant cost can be factored in the commercial bid submission.	The CSOC operations will be carried out from Chennai. However one resource is required at Mumbai DC site.

245	Period of Validity of Bids	22	a) Prices and other terms offered by Bidders must be firm for an acceptance period of nine (9) months from last date for submission of bids.	The prices are dependant on exchange rate variations. We request the bank to keep a shorter price validity of 4 months or include exchange rate variation of +/- 2% on the price submitted.	No change in RFP terms.
246	Termination	74	Termination for the convenience of bank: The bank may, at any point during the currency of this contract may terminate the contract by giving 30 days advance notice to the bidders without assigning whatsoever reason. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.	Incase of Termination for convinience by bank, we request the bank to compensate the bidder to the tune of cost already incurred by the bidder for the future AMC / ATS contracted with OEMs.	No change in RFP terms.
247	Insurance	91		The bidder can insure the equipments till the point of delivery. Since post-delivery these equipments will be in premise of the bank, we request the bank to insure the equipments. Hence kindly request the bank to delete this clause and limit insurance coverage only till delivery happens.	Necessary insurance of the goods supplied by the bidder for the damage, theft etc. till the delivery and installation at the delivery locations.
248	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have breach detection rate of more than 99% as per NSS lab Breach Detection Systems test report & the test report should be submitted	Considering latest cyber security trends & breaches, Requesting bank to emphasis on Breach Prevention rather than detection only. Requesting Bank to consider NSS BPS Breach Prevention system test report with Block rate of 99% & above as per latest NSS BPS Report.	No change in RFP terms.
249	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects without relying upon any external box solution like Firewall / NGFW / IPS/NGIPS/Web Proxy	Threats/IOC detected by Anti-APT & relevent intelligence should be shared across all security solutions including NGFW/NIPS for end-to-end protections at their level. Requesting bank revise clause to build shared intelligence architecture by integrating Anti-APT with NGFW.	No change in RFP terms.
250	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed Solution should have throughput of 2 GBPS, have the ability to support both inline and out-of-band detection and should cause limited interruption to the current network environment. The Bank reserves the option of using deployment as Inline or out-of-band.	Anti-APT solution performance is also depend on no. of files emulated per hour/day/month as undersize appliance can add latency in network. Need additional appliance sizing information such as no. of emails/internet users & total no. of emails with attachment received per day/month, similarly total no. of files download happens through proxy per day/month. This data will help to size right appliance considering the user & file emulation capacity of device.	The average number of mails sent and received for one month: Sent - 12,000 Received - 60,000
251	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack and the history of the movement of the malware in the network.	Kindly confirm if bank is also looking for Endpoint EDR agent solution for worksstations as part of this RFP. If Yes kindly share total no. of endpoints as well as OS flavours to consider.	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
252	Annexure 11.3 Anti – Advanced Persistent Threat / Performance	159	Solution should have a provision of 10G interfaces on Appliance proposed for Data ports.	Kindly confirm the no. of 10 GE interfaces to be considered ??	10G interface is not required currently. However the proposed solution should have provision of 10G interfaces on Appliance proposed for Data ports.
253	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed solution should have capability of horizontal scalability.	Bank should consider Anti-APT in HA pair per site DC/DR which will protect bank network & traffic will not be allowed without inspection even in case of device failure.	No change in RFP terms.
254	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed Solution should be address HTTP,HTTPS,SMTP,SMTP CIFS, FTP and other protocols	Requesting bank to add on-box SSL inspection support to prevent threats coming through SSL or polymorphic channel. Requesting Bank to add specification as "Proposd Soluton should support on-box SSL inspection feature to prevent attack originating from SSL & Polymorphic Channel."	No change in RFP terms.

255	Annexure 11.3 Anti – Advanced Persistent Threat/Endpoint Detection and Response	160	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf,.jpg, .dll, .sys, .com and .hwp	Requesting bank to delete support for .chm & .com file-type as it's avoiding renowed vendor to participate. Kindly confirm if it is acceptable to be added as future enhancement.	No change in RFP terms
256	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Bank has asked for Multi-layer security methodolgy which includes Anti-Virus & Anti-bot along with Sandboxing. MAC & linux based malwares can be detected through windows platform based APT using multi-inspect engine & threat intel from cloud. Requesting bank to allow only Windows platforms & not both which disallows renowed vendor from RFP participation.	No change in RFP terms
257	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Mobile malware come as .apk file & requires mobile specific ennviornment to emulate it. Kindly confirm if Bank is looking for separate Mobile solution as part of Mobile Security in this RFP ? If Yes, Kindly share the total no. of Mobile devices to be considered ??	There is no separate requirement for mobile security solution. However, the solution should support monitoring of mobile malwares for the connection originating from the mobile devices.
258	Annexure 11.3 Anti – Advanced Persistent Threat	161	The proposed solution should Block and hold file from spreading across all endpoints i.e. prevent lateral movement	We recommend bank to consider Endpoint EDR agent solution as part of this RFP which will protect lateral movements irrespective of Endpoint location such as online or offline (Roaming Laptops)	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
259	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	161	The solution should support CLI, and must be administered through a web based console using SSH/HTTPS. Should support AAA for role based administration	Considering the huge CVE list of Browser exploits & vulnerabilities getting discovered every year. Requesting Bank to consider agent based console as more secure & fastest configuration mode. Requesting to add software console based configuration mode as well. Requesting Bank to revised clause as "The solution should support CLI, and must be administered through a web based/agent based console using SSH/HTTPS. Should support AAA for role based administration	No change in RFP terms.
260	Annexure 11.1 Security Information and Event Management	142	#1. The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope	As per our understanding "Propose solution should be appliance based and separate hardware for collection, loging and correlation". Is our understanding correct?	The interpretation appears to be correct. The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module
261	Annexure 11.1 Security Information and Event Management	142	#6. Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	As per our understanding "Propose hardware should be capable to handle sustained 20,000 EPS from Day 1 ". Is our understanding correct?	The bidder has to provide SIEM license for 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
262	Annexure 11.1 Security Information and Event Management	144	#29. The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis.	Please share Network Throughput to size Packet Capture solution. Ex: " Packet capture solution should support 1 Gbps traffic and store Raw Packet for 7 days and Meta for 30 Days "	The bank currently has network throughput of 10 Gbps traffic.
263	Annexure 11.1 Security Information and Event Management	148	#98. System should have capacity to maintain the logs for 90 days on Tier I storage and older logs should be archived on Tier II storage and Tier 3 storage	As per our understanding storage should be sized for 10,000 EPS from Day 1. Is our understanding correct?	The interpretation appears to be correct. Please refer section 4 Scope of Work.
264	Annexure 11.1 Security Information and Event Management	146	The solution must have the ability to capture network traffic and import PCAP files.	It is always receommended to maintain the sanctity of logs for the SIEM solution by not importing any 3rd party logs in any of the formats. For such scenarios, other tools are recommended. Please explain the reason for importing the PCAP files to the SIEM. Moreover, this clause appears to be favoring a single vendor, hence, in order to promote fair competition this clause should be removed.	The proposed solution should have mentioned capability as this is an important requirement for the bank.

265	Annexure 11.1 Security Information and Event Management	149	The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents, permit upload of related evidences such as screenshots etc.	This is a core capability of the CRM / Incident management solution, hence, from SIEM solution perspective - please change the specification to the below statement: "The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents"	No change in RFP terms.
266	Annexure 11.1 Security Information and Event Management	143	The solution should have the capability to identify / remember frequently used queries and provide means for optimization of queries.	Please explain what do we mean and expect by the term "optimization of queries". Kindly change the statement to: "The solution should have the capability to identify / remember frequently used queries"	The solution should be agnostic to optimize the queries.
267	44	4.5 - H	The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement	License , Hardware & software should be sized for 2000 devices from day 1? 1 Device = 1 IP , Our Assumption is correct?	Yes.
268	44	4.5 - i	The Bank has offices at around 80 locations in addition to the DC and DR. Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, Bank has placed order for implementation of SD-WAN based IP MPLS network. The routers at the locations will be replaced with SD-WAN CPEs. The proposed solution should be able to capture logs from the CPE's installed at the locations. The Bidder's proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period	Please share the SD-WAN vendor details. What is the outcome/usecases bank are expecting with integrating SD-WAN solution? The proposed solution should be able to capture logs from the CPE's installed at the locations.----- Ideally Logs Capture is the feature of SIEM/Syslog solution , Request you to clarify, what are the expected outcome from NAC?	The vendor for SD-WAN currently is Sify. The usecase expected here is visibility and profiling.
269	50	z	OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.	Bidder will be the implementation & sustainance partner for bank , Request you to repharse it "Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation. "	The Bidder would be the single point of contact. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.
270	166	12	The solution should support existing third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM.	Please highlight the use case wrt all third party hardware/software. For exact boq sizing vendor details are must, Integration outcome is require from day 1? What all use cases/Outcome bank is expecting with integrating all the tools?	The hardware/software/devices/appliances are from the leading manufactures. The details will be shared with selected bidders.
271	167	30	The NAC Solution should support agentless , agent base & Desolvable agent mode	It is important for bank to check posture complaince with all the deployement mode, request you to repharse it as " The NAC Solution should support agentless , agent base & Desolvable agent mode for all the feature listed in technical compliance sheet (i.e discovery , profiling , posturing , access control & remediation.)"	No change in RFP terms.
272			Additional Query	Provide Network Infrastructure details (Like Total Number of switches , Routers, Wireless , Firewall etc)	Refer Annexure 11.7. The further details will be shared with the selected bidder.
273			Request addition	For Bank there are many IOT(Printers , Scanners , IP phone , IP camera , cheque scanning machine) devices connecting on to the enterprise network , its very important to include IOT posture assesment , The solution should be able to identify all network devices such as routers, switches, IOT's devices using factory default or Weak/common credentials as part of IOT Risk Assessment.	This is to be taken care in Vulnerability Assessment and Penetration Testing services.

274			Request addition	The NAC solution should support bank existing network infrastructure i.e Managed & unmanaged swiches to block or limit the non-complied and rough devices behind that.	No change in RFP terms.
275			Request addition	The solution should provide complete inventory of applications, processes, Services and open ports on all the endpoint.	No change in RFP terms.
276			Request addition	The solution should provide visibility into IPv6 enabled endpoints.	Separate clause has been added. Please refer to Corrigendum - 2.
277	Clause 6.17. Termination	74	Termination for the convenience of bank The bank may, at any point during the currency of this contract may terminate the contract by giving 30 days advance notice to the bidders without assigning whatsoever reason. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.	We request that any termination for convenience should be done only after providing 90 days written notice to the Bidder. Further, in case of termination for convenience, Bank shall also agree to pay, at a minimum: (i) all invoices issued by Dimension Data for the deliverables prior to the termination date; (ii) costs for performing or supplying deliverables as at the date of the termination notice; and (iii) costs that may be incurred by Dimension Data, which it is unable to mitigate or recover.	No change in RFP terms. SIDBI will pay the service fees in respect of the services delivered up to the effective date of termination as applicable / eligible and approved by the competent authority of the Bank deducting penalties if any.
278	6.17.2 Termination	74	The Selected bidder shall have right to terminate only in the event of winding up of the Bank.	We request deleting the above clause, as the same is arbitrary	No change in RFP terms.
279	6.22. Audit	77	The bidder shall allow the Bank, its authorized personnel, its auditors (internal and external), authorized personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the services including Hardware, Software provided to the Bank and CSOC operations under this RFP and the bidder shall extend all cooperation in this regard.	Please confirm that any audit shall be done with prior written notice to Bidder and should be restricted to the information and documents in relation to the services provided. Further, such audit shall be subject to the "Confidentiality" obligations upon the Bank, its auditors, employees making such audit. Also, we request confirmation that Bidder shall not be required to disclose its financial information, profits, books of accounts, costs breakups etc. and audit shall be strictly restricted to the services provided by the Bidder to the Bank.	No change in RFP terms.
280	6.25. Limitation of liabilities	80	The aggregate liability of bidder / service provider, arising at any time shall not exceed the total contract value.	We request that Liability of the Bidder be capped to the Annual Value of the Contract. Also, please clarify that the clause on IPR Infringement is related to the services provided by the Bidder and does not relate to the OEM Products/equipment supplied by the Bidder, where Bidder is not the OEM.	No change in RFP terms.
281	6.28 Resolution of Disputes	83	Additional Query	We request that Arbitration be conducted as per the Arbitration & Conciliation Act and Parties shall mutually appoint a sole arbitrator as per the Act.	No change in RFP terms.
282	6.32. Negligence	85		Please confirm that termination for default shall take place after providing written notice of 30 days to the Bidder and upon Bidder failing to cure such default within the notice period.	No change in RFP terms.
283	Annexure 8.10 Pre-Contract Integrity Pact 7. Fall Clause	127	The BIDDER undertakes that it has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.	While we agree to execute the pre-contract integrity pact, however, we request deletion of the Fall Clause. Please appreciate that prices are dependent on various factors, including, passage of time, discounts received from the OEM, quantity and location of supply, rate if LD, penalties and other contractual risks. Bidder is unable to accept the Fall Clause.	No change in RFP terms.

284	6.24. Indemnity	78	Additional Query	We request that provisions related to Indemnity be restricted to the following: Third party indemnification claims arising from breach of confidential information, Third party indemnification claims arising from infringement of IPR in respect of the Services provided by Bidder Further, as per the standard legal procedure, the clause on Indemnity should capture the following: a. IDBI should promptly notify Bidder in writing about any such third party claim b. IDBI should take all practical steps to mitigate any loss arising out of such third party claims c. IDBI should not make any admission, compromise or settle the claims without the prior written consent of the Bidder and should allow the Bidder to control and conduct proceedings (including settlements) arising from such third party claims d. IDBI should provide the Bidder with all assistance as it may reasonably require in such proceedings.	No change in RFP terms. Please refer to section 6.24 Indemnity of the RFP.
285	3.2 - Objective # i	32	Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.	Services would be provided in compliance with the applicable laws. Is there any special reason for referring IT Act 2000 in the provision? Please clarify.	The bidder has to support the CSOC solutions for the Bank against all the compliance standards maintained by the Bank.
286	4.8.3 - Implementation & Integration #bb	50	Bidder shall provide list of licenses to be procured, also maintain the inventory database of all the licenses and the updates installed. Also, the licenses should be in the name of Bank.	What kind of licenses SIDBI expects bidder to maintain and procure here? Please clarify.	The bidder is expected to maintain a asset inventory for all the hardware/software/appliance/license/devices provided as part of this RFP.
287	4.8.3 - Implementation & Integration #gg	51	CSOC setup / infrastructure may be subjected to audit from Bank and/or third party and/or regulatory body. It shall be responsibility of the Bidder to co-operate and provide necessary information and support to the auditors. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty.	Bidder requests bank to specify the exact nature of the audit. Bidder cannot permit any one to audit bidder's network or network equipment as it is a shared facility with other customers. Further vendor propose that any audit be conducted after providing not less than 30 days' prior notice to vendor and the audit be made subject to the auditors entering into a confidentiality agreement with bidder. The audit shall be conducted not more than once in a calendar year and remote hands fee be applicable to the same. Further the audit should not exceed a time duration of 4 hours (in any case should not exceed 8 hours) at any given instance. “Remote Hands Fee(s)” shall mean bidder's standard rates for any facility under audit and are intended to compensate bidder's costs for providing bank access to bidder’s facilities and personnel during the audit	The bidder has to support the CSOC solutions for the Bank against the security audits and compliance standards maintained by the Bank.
288	6.13-Terms of Payment & Payment Milestones	70	Terms of Payment and Payment Milestones The payments for services will be released on quarterly basis as arrears for all the implemented solutions and services.	Request SIDBI to change payment terms to quarterly in advance	No change in RFP terms.
289	6.13-Terms of Payment & Payment Milestones - Point # m	71	The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the Bank.	Instead of withholding of Bidders payments by Bank, we request Bank to incorporate following clause: In the event Bank disputes in good faith any portion of Bidder’s invoice, Bank must pay the undisputed portion of the invoice and submit a written claim for the disputed amount, together with all information relevant to the dispute, including the reason for the dispute. All disputes must be submitted to the Bidder within forty-five (45) days of receipt of the first invoice for the applicable charges. Bank acknowledges that it is reasonable for the Bidder to require Bank to dispute charges within that time, and Bank therefore waives the right to dispute any charges not disputed within the time frame set forth above.	No change in RFP terms.
290	6.17 - Termination Point #1	74	Termination for non-performance (not meeting SLA)	What would be the defect cure period available to the bidder to cure the defect?	30 days.

291	6.17 - Termination Point #3	74	The bank may, at any point during the currency of this contract may terminate the contract by giving 30 days advance notice to the bidders without assigning whatsoever reason. In this event, termination will be without compensation to the Bidder, provided that such termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.	We request SIDBI that in case of termination for convenience by SIDBI, SIDBI shall pay the service fees in respect of the services delivered up to the effective date of termination and the following amounts: (i) an amount equal to the total of any and all waived installation charges as reflected on the terminated order(s), (ii) an amount equal to one hundred percent (100%) of the service fees payable for the unexpired remainder of the order period plus (iii) any documented third party expenses not covered by (i) and (ii) above that are incurred by bidder in respect of the terminated order (including any local loop charges).	No change in RFP terms. SIDBI will pay the service fees in respect of the services delivered up to the effective date of termination as applicable / eligible and approved by the competent authority of the Bank deducting penalties if any.
292	6.18 - Applicable Laws	76	Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this Tender and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees / officers / resource / personnel / representatives / agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.	Bidder could not take the responsibility to notify Bank regarding the laws which could be applicable on the Bank while using the services. Bank has to conduct due diligence in order to find out the laws that are applicable on Bank while use of services or for conducting its business.	No change in RFP terms.
293	6.23 - IPR Infringement	78	IPR Infringement	Bidder request SIDBI that the Bidder's liability for infringement of intellectual property rights (IPR) should be limited. As for the deliverables created by Bidder, Bidders indemnity should be capped to the immediately preceding 12 months of charges collected by Bidder under the order in which the liability has arisen.	No change in RFP terms.
294	6.24 - Indemnity	78	Indemnity	Indemnity claimed by Bank is very broad. Bidder would like to propose the following for consideration of Bank: Bidder shall indemnify and keep indemnified Bank from third party claims arising from damage to tangible property, loss of life or personal injury caused due to Bidder's gross negligence or willful misconduct.	No change in RFP terms.
295	6.25 - Limitation of Liabilities	80	Limitation of liabilities	The exceptions mentioned herein would result into claim of indirect or consequential damages for claims related to IPR or for general indemnity. This is not acceptable. Bidder request to cap its overall liability to the aggregate of 12 month of the charges, with exclusion of indirect or consequential damages, collected by Bidder under the order in which such liability has arisen. Bidders sole liability and Bank's sole remedy for damages relating to services is limited to any applicable credit allowances/penalties due.	No change in RFP terms.
296	6.26 - Confidentiality	80	Confidentiality	SIDBI at any time may opt for injunctive relief. Indemnity for confidentiality breach is not acceptable to bidder.	No change in RFP terms.
297	6.32 - Negligience	85	Negligence	Appropriate amount of penalties/liquidated damages have been imposed by the Bank for service breach. In the presence of such financial implications cost for replacement services and/or to compensate the Bank for loss resulted from such breach as mentioned in the provision is not acceptable and must be omitted from the RFP. Further the Bidder would be responsible for damage to tangible property caused due to bidder's gross negligence and any consequences referred in this section are not acceptable to the bidder.	No change in RFP terms.

298	6.33 - Miscellaneous Point # e	86	Bidder shall indemnify, protect and save SIDBI against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting directly or indirectly from an act or omission of Bidder, its employees, its agents, in the performance of the services provided by contract, infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided by Bidder as part of the delivery to fulfill the scope of this project.	Please refer to comments made under section 6.23, 6.24 and 6.25.	No change in RFP terms.
299	Annexure 8.10 - Integrity Pact - #7: Fall Clause	127	The BIDDER undertakes that it has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded	Benchmarking of prices is not acceptable. Bidder request to omit such process since the prices have been well negotiated between the parties and will continue to remain firm during the terms of the Contract keeping in view the current market situation.	No change in RFP terms.
300	Annexure 8.10 - Integrity Pact - #9: Facilitation of Investigation	128	9. Facilitation of Investigation In case of any allegation of violation of any provision of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.	SIDBI will have access to their books of accounts only and documents available in public domain.	No change in RFP terms.
301	6.22 - Audit	77	Audit: The bidder shall allow the Bank, its authorized personnel, its auditors (internal and external), authorized personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the services including Hardware, Software provided to the Bank and CSOC operations under this RFP and the bidder shall extend all cooperation in this regard.	Request Bank to change the clause to have access to Bidder's documents and reports available in public domain	No change in RFP terms.
302	4.1 Security Information and Event Management	39	J) The logs collected by the SIEM log collector should be replicated across primary Data Center and Disaster Recovery location. The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder.	How much RPO / RTO expected between DC & DR by SIDBI?	The CSOC operations need to maintain SLA and uptime as per Section 7 of the RFP. Yes
303	B. Storage	39	a) The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs for up to 9 months and offline storage for storage of logs for up to 6 years. Total 7 years log must be available. The bidder is responsible for sizing the storage adequately based on the sustained EPS of 5,000 with 50% overload at the peak usage, scalable up to sustained level of 10,000 EPS.	Bidder understanding is that 3 Months data online, 9 Months on tier 2 storage and 6 Years on offline media. Does 3 months data required to be SSD, SAS & Tape respectively ? Please clarify if any specific IOPS requirement.	The interpretation appears to be correct. The vendor needs to size the storage to maintain the SLA and uptime mentioned in the RFP. Please refer to Section 4 Scope of Work and Section 7 of RFP.
304	B. Storage	39	The bidder is responsible for automated online replication of logs from DC to DR for redundancy. The solution should be capable of automatically moving the logs from device to archival storage based on the ageing of the logs. The storage should have “Write Once Read Many (WORM)” / Encryption/ Index and Search/ Retention and Disposal functionality. The storage should have the option to support backup on tape library. For DC-DR replication, the solution should also have the capabilities to replicate the logs in real-time and should have configuration for scheduled replication whenever required.	Is it mandatory to provide tape based archival solution OR Bidder can propose B2D-to -Disk -to DR replication solution.	No change in RFP terms.

305	B. Storage	40	The bidder will have to make the archival logs available within 24 hours and live logs in real time of a request made by the bank. This request for retrieval of archival logs would be considered as a Medium Priority incident. If the bidder fails to provide the required logs within 24 hours, then penalties applicable for Medium Priority incidents would be levied.	Restoration of arcival logs within 24 Hrs. from offsite tapes will be challenge. Please considered Disk to Disk based backup and for long term archival solution. Please confirm.	No change in RFP terms.
306	4.8. Other General Requirement	46	e) The bidder needs to propose only Veritas backup solution for backups.	Please relax the clause which is limiting to single vendor. Request SIDBI to consider other backup tools which has lot more capabilities built and price advantages	No change in RFP terms.
307	4.8.3. Implementation & Integration	50	x) The Bidder would be responsible for installation, testing, commissioning, configuring, warranty and maintenance of the system. The bidder will also provide necessary support and coordination for conducting BCP/DR drill and testing as per SIDBI BCM and IT security policy.	How many DR-Drill is expected in a year?	The details will be shared with selected bidders.
308	General Query	N.A.	N.A.	Can bidder propose virtulization Hypervisor software to virtualize all the proposed servers for resource optmization? Does SIDBI has any existing virtualization footprint ?	The bidder can only propose VMWare as part of virtualization provided there are no restrictions / technical challenges from other partner OEMs for the proposed security solutions to be implemented. However, all the required software/hardware/licenses as part of virtualization needs to be provided by the bidder. Please refer section 4 "Scope of Work" of the RFP.
309	4.6-VAPT Information and Remediation Services	44	Bidder should execute this service on quarterly basis	Can bidder propose virtulization Hypervisor software to virtualize all the proposed servers for resource optmization? Does SIDBI has any existing virtualization footprint ?	The bidder can only propose VMWare as part of virtualization provided there are no restrictions / technical challenges from other partner OEMs for the proposed security solutions to be implemented. However, all the required software/hardware/licenses as part of virtualization needs to be provided by the bidder. Please refer section 4 "Scope of Work" of the RFP. However, the VAPT need to be performed by resources onsite.
310	4.6	44	Bidder should execute this service on quarterly basis	As per Section 7.3, Vulnerability Assessment required Monthly basis & Bank is having own tool. Penetration testing have to do Quarterly basis. Please confirm.	The bidder has to bring in their own tools for VAPT services. The bidder has to provide VAPT service to Bank on quarterly basis as and when required.
311	7.3 -SLA (VA)	99	The bidder is expected conduct Vulnerably Assessments by using existing tools (Beyond Trust Retina CS, NESSUS, Nipper) 1) To be conducted for identified devices once every month based on a calendar documented in coordination with the bank to ensure that business operations are not impacted	Please confirm, bank is having own tool to conduct VA or bidder suppose to bring own tool.	The bidder has to bring in their own tools for VAPT services.
312	3.2 - Objective #j	32	Provide forensics support as per the requirement of Bank in case of any incident or as and when required	Please share no. of incidents yearly to do foresics against incidents.	The support in forensics should be irrespective of numbers, the support in forensics will be required in case of incident, as and when required.
313	3.2 - Objective #o	32	Hardening of devices needs to be performed for new devices as part of implementation	IS bank having SCD framework to do hardening od devices or bank expect to create new SCD process by bidder.	The bidder is required to comply with bank's policy and adhere to the defined industry benchmarks for all devices.
314	4.1 - SIEM	39	The logs collected by the SIEM log collector should be replicated across primary Data Center and Disaster Recovery location. The bidder will be responsible for providing P2P link for the log replication collected by SIEM log collectors across primary DC site and DR site. The sizing and requirement of all such links will be the responsibility of bidder	As per section 4, Bank require only collector layer at DR so there is no logger required at DR. How we can repliplicatio logs between DC & DR.	The bidder is expected to replicate the logs from DC to DR not only for SIEM, but for other components as part of this RFP.
315	4.1 - SIEM	39	The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs for up to 9 months and offline storage for storage of logs for up to 6 years. Total 7 years log must be available. The bidder is responsible for sizing the storage adequately based on the sustained EPS of 5,000 with 50% overload at the peak usage, scalable up to sustained level of 10,000 EPS.	As per my understanding. Retaintion period of logs are "3 Months online on Logger", "9 Months on Nearline Storage" & "6 Years on Tape". Total 7 Years of logs available. Please confirm the same.	The interpretation appears to be correct. The SIEM should be able to maintain 3 months of logs on-box. In addition, the bidder should provide for near line storage i.e. secondary storage for archiving logs for up to 9 months and offline storage for storage of logs for up to 6 years. Total 7 years log must be available.
316	4.1 - SIEM	39	The bidder is responsible for automated online replication of logs from DC to DR for redundancy.	As per section 4, Bank require only collector layer at DR so there is no logger required at DR. How we can repliplicatio logs between DC & DR.	The bidder is expected to replicate the logs from DC to DR not only for SIEM, but for other components as part of this RFP.

317	4.1 - SIEM	39	a) Offsite storage facility is also required for additional 6 years in Tape Library with minimum of LTO 6.	As per section 4.1, bank stated "For Tape Backup/SAN required Tape and other Hardware should be provided by Bidder. Bank will provide the storage safe only to keep the Tape. The bidder will be responsible for tape movement securely to the offsite storage site." Both statements are contradiction to each other. Please Confirm is bank will provide storage safe t0 preserv tapes.	Bank will provide storage safe to keep the tape.
318	4.1 - SIEM	40	As per section 4.1, bank stated "For Tape Backup/SAN required Tape and other Hardware should be provided by Bidder. Bank will provide the storage safe only to keep the Tape. The bidder will be responsible for tape movement securely to the offsite storage site." Both statements are contradiction to each other.	If Bank is providing Storage safe, then Tape offsiting is not bidder responsibilty. Please confirm.	No change in RFP terms.
319	4.4 - Firewall Analyzer	43	a) Bidder should execute this service on monthly basis / whenever required due to changes in network / system configuration	Is bank looking Firewall analyzer as a service model or dedicated tool to be deployed on premise?	Dedicated tool to be deployed on premise.
320	4.8- Other General Requirement	46	a) The bidder needs to propose only Veritas backup solution for backups.	Please confirm, bank is using which Veritas tool Netbackup or Backup Exec?	Veritas Netbackup for Data Center and DR Site.
321	11.3 - Anti APT	160	Solution must have the capability to analyze large files and Must be able to support minimum 100MB file size	File size limit should be reconsidered as file more than 15-20MB are not allowed to be downloaded from internet for normal users. Also processing of 100Mb file in sandbox can take time to analyze & can affect user experience.	No change in RFP terms.
322	11.3 - Anti-APT	158		Kindly share Existing Endpoint Protection, Web protection & Email security solution details to craft proper intergration of Anti-APT solution with existing security solutions.	Refer to section 3.3 of the RFP. SIDBI has implemented Symmantec for existing endpoint protection, Blue Coat proxy for Web protection and Microsoft Exchange Online Protection for email security solution.
323	4.2 - PIM	42	SIDBI intends to implement a Privileged Identity Management solution to protect, monitor, detect, alert and respond to privilege account escalation activity.	Please provide the details of infrastructure, devices apart from SIEM that need to be integrated with PIM solution. Also inform the number of administrators from banks side that will covered under required PIM solution. These details are required to right size the PIM solution	The number of devices to be integrated with PIM is 200. The number of privileged users to be integrated with PIM solution are 70.
324	4.4 - Firewall Analyzer	43	SIDBI intends to have Firewall Analysis to analyze and optimize policies/configuration of its multiple firewalls currently installed at DC & DR.	Please share the number of firewall to be covered under this solution	Initially Approximately 15
325	4.5 - NAC	43	The Bank intends to procure a Network Access Control solution which is an automated security control platform that can monitor and control everything on the network—all devices, all operating systems, all applications, all users. The solution shall let employees and guests remain productive on the network while critical network resources and sensitive data remain protected.	Please provide the number of users also in bank environment applicable for NAC solution. This will help to right size NAC solution along with number of devices as some users might have multiple devices tagged to them	Please refer Annexure 11.7
326	Annexure 10.2 - Commercial Bid Format	138	Commercial Bid Format: Bank will calculate NPV on the 2nd and 3rd year quoted as part of Annual Cost using the formulae below: Net Present Value of Current Year = Cost of Respective Year / (1 + Discount Rate in %) Year-1 The discount rate to be considered for above would be 8.38% per annum	Please provide example of how TCV will be calculated.	Please refer to Annexure 10.2 of the RFP.
327	7 (c) - Delivery penalty	95	Delivery Penalty: The Liquidated damages to be recovered under above clauses shall be restricted & capped to 10% of the total value of the order for each year independently during the contract period.	Request bank to change it to following clause: The Liquidated damages to be recovered under above clauses shall be restricted & capped to 3% of the TCV of the order for each year	No change in RFP terms.
328	7.1 -Liquidated damages for delay in Delivery and Installation of Hardware and Software	95	Liquidated damages for delay in Delivery and Installation of Hardware and Software 1. LD at the rate of 1% per week of the cost quoted against each of respective item as mentioned in Commercial Bid for items not delivered will be levied per week or part thereof (on pro rata basis for the no. of days) and deducted against bills submitted 2. In case of delay in integration beyond three months, LD at the rate of 1% per month of the cost quoted against SIEM as mentioned in Commercial Bid will be levied per month for the no of days of delay (on pro rata basis for the no. of days) and deducted against bills submitted.	Request to keep penalty of every component to max cap of 5% of cost.	No change in RFP terms.
329	7.2 - LD for not maintaining uptime	96	7.2. Liquidated damages for not maintaining uptime	Request to keep cumulative penalty of every component to max cap of 5% of total cost.	No change in RFP terms.

330	7.2 (l) - Liquidated damages for not maintaining uptime.	97	For the L1, L2 and L3 resources for the leave of absence. LD will be levied for any absence for which no substitute is arranged by the Service Provider as per defined in the below table: • L1 Resource - Rs.2000/- per day maximum Rs.10000/- per month • L2 Resource - Rs.2500/- per day maximum Rs.15000/- per month • L3 Resource - Rs 3000/- per day maximum Rs 20000/- per month	Request to keep penalty for each resource to max cap of 5% of monthly cost of each resource.	No change in RFP terms.
331	7.3 - SLAs and LD	98	7.3. SLAs & Liquidity Damages for CSOC Operations	Request to keep cumulative penalty of every component to max cap of 5% of quarterly cost.	No change in RFP terms.
332	4.1 SIEM (B - Storage #a)	39	The SIEM should be able to collect logs from the devices/applications/databases etc. mentioned by bank as per the Annexure 11.7 including the solutions deployed as part of this RFP. It should be able to collect the logs from devices from geographically dispersed locations.	As per tech spec 140 The offered solution should include vulnerability details with updates from a known vulnerability database like NVD (National Vulnerability Database) or similar databases. In this specification you have asked for log collection from geographically dispersed locations. We would like to know whats the EPS expected from other locations other than DC & DR. If appliance based solution has to be proposed then then pls help us with these details to size the appliance or please help to change the spec to appliance/software.	The bidder has to provide SIEM license for 10000 EPS from day 1.
333	4.1 SIEM (A - Solution Implementation) #k	39	k) The bidder should provide SIEM license for 10000 EPS from day 1.	In storage section; storage is asked for 5000 sustained and 10000 peak EPS. Is SIDBI looking for license also for 5000 sustained EPS and 10000 Peak EPS? Apart from storage license should be mandatorly asked based on sustained and solution should be able to handle double the capacity to handle peak EPS and no events should be dropped. Hence we request SIDBI to change the specs to below: The bidder should provide SIEM license for 5000 sustained EPS and 10000 peak EPS and no events should be dropped, none of the functionalities should be stopped even in case SIEM cross peak EPS during data burst or attack scenarios.	The bidder has to provide SIEM license for 10000 EPS from day 1 and bidder has to consider the sizing accordingly.
334	Annexure 11.1 - SIEM #1	143	The proposed solution should be an appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope.	As SIDBI has asked for log collection from various geograhpical locations; with this requirement software based solutions are very flexible and can be deployed anywhere when required. Hence we request SIDBI to change the spec to below: The proposed solution should be an software/appliance with a clear physical or logical separation of the collection module, logging module and correlation module. It should support log collection, correlation and alerts for the number of devices mentioned in scope.	No change in RFP terms.

335	Annexure 11.1 - SIEM #6	143	Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	In storage section; storage is asked for 5000 sustained and 10000 peak EPS. Is SIDBI looking for license also for 5000 sustained EPS and 10000 Peak EPS? Apart from storage license should be mandatorly asked based on sustained and solution should be able to handle double the capacity to handle peak EPS and no events should be dropped. Hence we request SIDBI to change the specs to below: The bidder should provide SIEM license for 5000 sustained EPS and 10000 peak EPS and no events should be dropped, none of the functionalities should be stopped even in case SIEM cross peak EPS during data burst or attack scenarios.	The bidder has to provide SIEM license for 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
336	Annexure 11.1 - SIEM #14	144	The proposed solution shall allow bandwidth management, rate limiting, at the log collector level.	This is a very important feature and along with this feature it is mandatory to have event aggregation, event filtering etc also on log collection level. This will benefit SIDBI to optimize storage, events reaching correlation engine. We request the to change to below: The proposed solution shall allow bandwidth management, rate limiting, filtering, aggreagation, at the log collector level.	No change in RFP terms.
337	Annexure 11.1 - SIEM #21	144	It should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.	We would like to understand what exactly SIDBI would like to do here?	The proposed solution should have feature for importing/exporting the raw logs.
338	Annexure 11.1 - SIEM #27	144	The proposed solution should be able to capture critical fields of information in the original event data, logs and alert messages and normalize / parse them into a common standard event schema for further analysis, troubleshooting and other data processing needs.	Log events should be normalized to common event schema at the log collection layer so that log management layer should be doing log management only and not parsing. Hence we request to change the specs to below: The proposed solution should be able to capture critical fields of information in the original event data, logs and alert messages and normalize / parse them into a common standard event schema in log collection level for further analysis, troubleshooting and other data processing needs	The proposed solution should be able to capture critical fields of information in the original event data, logs and alert messages and normalize / parse them into a common standard event schema for further analysis, troubleshooting and other data processing needs.
339	Annexure 11.1 - SIEM #29	144	The proposed solution should collect log & support forensics with added context and threat Intelligence and provide complete visibility through packet inspection and analysis.	Is SIDBI looking for full packet capture? How many segments are available for packet capture? How many days packet capture data has to be kept? All major SOC RFP's have asked dedicate and separate packet capture solution as packet capture solution technical specifications are not covered in two specs. Hence we request SIDBI to have dedicate packet capture specs or revove this from RFP as this is also specific to one particular vendor.	The proposed solution should have mentioned capability as this is an important requirement for the bank.
340	Annexure 11.1 - SIEM #40	146	The proposed solution should provide the ability to aggregate an analyze events based on a user specified filter.	This feature should be available from log collection level only. Hence we request to chagne the spec to below: The proposed solution should provide the ability to aggregate an analyze events based on a user specified filter in log collection level.	No change in RFP terms.
341	Annexure 11.1 - SIEM #54	146	The proposed Solution should be able to filter the captured packets based on layer-2 to layer-7 header information. The solution should also provide ability to reconstruct data payload.	Is SIDBI looking for full packet capture? How many segments are available for packet capture? How many days packet capture data has to be kept? All major SOC RFP's have asked dedicate and separate packet capture solution as packet capture solution technical specifications are not covered in two specs. Hence we request SIDBI to have dedicate packet capture specs or revove this from RFP as this is also specific to one particular vendor.	The proposed solution should have mentioned capability as this is an important requirement for the bank.

342	Annexure 11.1 - SIEM #55	146	The solution must have the ability to capture network traffic and import PCAP files.	Is SIDBI looking for full packet capture? How many segments are available for packet capture? How many days packet capture data has to be kept? All major SOC RFP's have asked dedicate and separate packet capture solution as packet capture solution technical specifications are not covered in two specs. Hence we request SIDBI to have dedicate packet capture specs or revove this from RFP as this is also specific to one particular vendor.	The proposed solution should have mentioned capability as this is an important requirement for the bank.
343	Annexure 11.1 - SIEM #85	148	Administrators should be able to view correlated events, packet level event details, real-time raw logs and historical events through the dashboard.	Is SIDBI looking for full packet capture? How many segments are available for packet capture? How many days packet capture data has to be kept? All major SOC RFP's have asked dedicate and separate packet capture solution as packet capture solution technical specifications are not covered in two specs. Hence we request SIDBI to have dedicate packet capture specs or revove this from RFP as this is also specific to one particular vendor.	The proposed solution should have mentioned capability as this is an important requirement for the bank.
344	Annexure 11.1 - SIEM #93	148	The 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.	As SIDBI has asked for appliance based solution and has also asked to collect logs from multiple locations. Hence we request SIDBI to have SIEM either appliance/software option. Also please let us know if SIDBI is looking for SIEM in HA in DC and DR or HA in DC and standalone in DR or standalone in DC and standalone in DR.	Please refer Section 4 Scope of Work of RFP.
345	Annexure 11.1 - SIEM #127	151	The offered solution should store all logs in raw format as sent by the above devices. These raw logs should be time stamped and compressed before being written to the storage. The logs should be maintained in tamper proof condition and shall have proper integrity mechanisms to be in place for log security.	Raw logs should not be timestamped; normalized logs should be timestamped and time stamping should be done at each layer on SIEM right from log collection layer to correlation layer. Hence we request SIDBI to change it to below: The offered solution should store all logs in raw format as sent by the above devices. These raw logs should be normalized and time stamped and compressed before being written to the storage. The logs should be maintained in tamper proof condition and shall have proper integrity mechanisms to be in place for log security.	No change in RFP terms
346	Annexure 11.1 - SIEM #140	151	The offered solution should include vulnerability details with updates from a known vulnerability database like NVD (National Vulnerability Database) or similar databases.	All leading SIEM vendors integrate with vulnerability management solutions for vulnerability information associated to devices. Hence we request to change the specs to below: The offered solution should integrate with all leading vulnerability management solutions. which should include vulnerability details with updates from a known vulnerability database like NVD (National Vulnerability Database) or similar databases.	The feature should be available during implementation and configuration.
347	Annexure 11.4	163, Point number 10	The proposed solution should allow opening a Change Request for removing the Unused Rules and Covered rules directly from the analysis report for ease of operations. The removal of these rules should also be automatic irrespective of the firewall brand in case bank decides to procure change management module as well from the same OEM in near future.	Please confirm if SIDBI would like to procure the Firewall Change Management solution and whether that should be available from the day one during the Implementation?	The proposed solution should have mentioned capability.
348	Annexure 11.4	163, Point number 11	The proposed solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices	Please confirm total number of L3 Routers/Switches to build the network map automatically? Pls confirm total number of Physical and Virtual Firewall clusters/Pair?	The details will be shared with successful bidder.
349	Annexure 11.4	164, Point number 14	The proposed solution should have a change management capability and should support Bulk change request submission through Excel file	Please confirm if SIDBI needs Firewall change management capability also from the day one?	The proposed solution should have mentioned capability.

350	Annexure 11.4	165, Point number 26	The Proposed solution should have a scalability factor to discover and map the business applications and the associated logical connectivity with the underlying security policies. It should also be able to build the application flows based on the Firewall policies if required.	Please confirm what does scalability means? Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should be scalable and have mentioned capability if the bank requires in future.
351	Annexure 11.4	165, Point number 27	Solution should identify Blocked and allowed flows from an application perspective to enable application team to collaborate with the operations team	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
352	Annexure 11.4	165, Point number 29	The proposed solution should have a provision of decommissioning of business application. The decommissioning process should be fully automated and the rules should be removed automatically from the Firewalls only for that application which needs to be decommissioned. The system should also identify those rules which cannot be removed as those could be linked to other applications.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
353	Annexure 11.4	165, Point number 30	The proposed solution should be application centric and have a provision for server migration process. The process should be fully automated and should specify the inline applications and their logical connectivity which requires changes. The proposed system should even provision the necessary rules on the FW's automatically.	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm the number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
354	Annexure 11.4	165, Point number 31	The solution should provide an ability to verify the impact on business applications if the inline FW is down or a specific policy on the FW is blocking the application traffic	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
355	Annexure 11.4	165, Point number 32	The proposed solution should have a capability to map the Firewall configuration risks with the inline business applications. It should present the risks in the overall application context	Would Bank like to procure licenses from the day one to achieve the said functionality? If Yes, please confirm total number of internal business applications SIDBI has?	The proposed solution should have mentioned capability if the bank requires in future.
356	3.3 Current Information Technology Setup	Page 33, Point A	Data Centre and DR Site	Please confirm if the solution is required in HA-DR architecture or only at DC as a standalone solution?	Please refer Section 4 Scope of Work of RFP.
357	4.5 - NAC (H)	44	The Bidder is required to design & size the NAC solution. Currently Bank has approximately 1600 devices including laptops, desktops etc. which needs to be covered in this solution. The Bank envisages the increase in the number of such devices to 2000 during the next 3 years. The bidders proposed solution shall be sized to meet the 3 year requirement	License , Hardware & software should be sized for 2000 devices from day 1? 1 Device = 1 IP , Our Assumption is correct?	Yes.
358	4.5 - NAC (i)	44	The Bank has offices at around 80 locations in addition to the DC and DR. Each of these locations has one or two Cisco router(s) & one / more manageable switches. The switches are of heterogeneous make with majority of them being HP/Aruba. Further, Bank has placed order for implementation of SD-WAN based IP MPLS network. The routers at the locations will be replaced with SD-WAN CPEs. The proposed solution should be able to capture logs from the CPE’s installed at the locations. The Bidder’s proposed solution shall meet the Bank's requirement as described and should support heterogeneous environments till the end of contract period	Please share the SD-WAN vendor details. What is the outcome/usecases bank are expecting with integrating SD-WAN solution? The proposed solution should be able to capture logs from the CPE’s installed at the locations.----- Ideally Logs Capture is the feature of SIEM/Syslog solution , Request you to clarify, what are the expected outcome from NAC?	The vendor for SD-WAN currently is Sify. The usecase expected here is visibility and profiling.
359	4.8.3 (z)	50	OEM would be responsible for all technical support to maintain the required uptime through the Bidder. Initial installation, configuration and integration should be done by the OEM, through the Bidder. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required onsite support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.	Bidder will be the implementation & sustainance partner for bank , Request you to repharse it "Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. The Bidder would be the single point of contact. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation. "	The Bidder would be the single point of contact. Initial installation, configuration and integration should be done by the Bidder, through the OEM support. Bidder would be responsible for all technical support to maintain the required uptime through the OEM support. The Bidder should have necessary agreement with the OEM for all the required support for entire project period. Bidder should have back-to-back support with OEM during the total contract period for necessary support. OEM should review and certify the successful implementation.

360	Annexure 11.5 - NAC (#12)	166	The solution should support existing third party hardware/software such as Network switches, Wireless Access Points, VPN, Antivirus, Patch Management, Ticketing, SIEM, Vulnerability assessment scanners and MDM.	Please highlight the use case wrt all third party hardware/software. For exact boq sizing vendor details are must, Integration outcome is require from day 1? What all use cases/Outcome bank is expecting with integrating all the tools?	The hardware/software/devices/appliances are from the leading manufactures. The details will be shared with successful bidders.
361	Annexure 11.5 - NAC (#30)	167	The NAC Solution should support agentless , agent base & Desolvable agent mode	It is important for bank to check posture complaince with all the deployement mode, request you to repharse it as " The NAC Solution should support agentless , agent base & Desolvable agent mode for all the feature listed in technical compliance sheet (i.e discovery , profiling , posturing , access control & remediation.)"	No Change in RFP Terms
362	N.A.	N.A.	Additional Query	Provide Network Infrastructure details (Like Total Number of switches , Routers, Wireless , Firewall etc)	Refer Annexure 11.7. The further details will be shared with the successful bidder.
363	N.A.	N.A.	Point to be added	For Bank there are many IOT(Printers , Scanners , IP phone , IP camera , cheque scanning machine) devices connecting on to the enterprise network , its very important to include IOT posture assesment , The solution should be able to identify all network devices such as routers, switches, IOT's devices using factory default or Weak/common credentials as part of IOT Risk Assessment.	This is to be taken care in Vulnerability Assessment and Penetration Testing services.
364	N.A.	N.A.	Point to be added	The NAC solution should support bank existing network infrastructure i.e Managed & unmanaged swiches to block or limit the non-complied and rough devices behind that.	No change in RFP terms
365	N.A.	N.A.	Point to be added	The solution should provide complete inventory of applications, processes, Services and open ports on all the endpoint.	No change in RFP terms
366	N.A.	N.A.	Point to be added	The solution should provide visibility into IPv6 enabled endpoints.	Separate clause has been added. Please refer to Corrigendum-2.
367	3.2 Objective	32	Provide proactive threat intelligence and threat hunting.	Need more clarity on the scope of threat hunting as well as frequency etc.	The bidder has to provide Threat hunting service to Bank on quarterly basis.
368	3.2 Objective	32	Hardening of devices needs to be performed for new devices as part of implementation	Is SIDBI having templates based on certain framework which needs to be followed. Frequency of the exercise etc.	The bidder is required to comply with bank's policy and adhere to the defined industry benchmarks for all devices.
369	3.2 Objective	32	Support all kind of audits during contract period	Please specify the type of audits expected to perform. Frequency.	The bidder has to support the CSOC solutions for the Bank against the security audits and compliance standards maintained by the Bank.
370	3.2 Objective	32	Ensure future integration with new applications and devices as part of CSOC operations during contract period	Please share the list of new technologies to be added during contract Period.	The details will be shared with the selected bidder as and when applicable
371	4.1 Scope of Work, SIEM	38	Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.	No. of users and asset base for solutioning the tool.	The number of incidents are irrespective to number of users. Please refer scope of work and annexure 11.7
372	4.2 Scope of Work, PIM	42	SIDBI intends to implement a Privileged Identity Management solution to protect, monitor, detect, alert and respond to privilege account escalation activity.	No of users license required.	The number of devices to be integrated with PIM is 200. The number of privileged users to be integrated with PIM solution are 70.
373	4.6 Scope of Work, VAPT Information and Remediation Services	45	The Bidder is to bring his own VAPT tools for testing purpose and obtain required approval for conducting the same.	In the SLA segment, SIDBI has mentioned to use existing tool, however, here the ask is to bring own tool. Please confirm, if SIDBI would provide the tool or we would have to bring our own.	The bidder has to bring in their own tools for VAPT services.
374	Annexure 8.2 - Pre-Qualification Criteria for Bidder	104	Point 3 - The proposed bidder should have presence in India and should be able to support project in India (Mumbai and Chennai) during the contract period.	Bidder should have 2 operational SOCs in India.	No change in RFP terms
375	Annexure 8.2 - Pre-Qualification Criteria for Bidder	104	Point 4 - The bidder should have atleast 200 crores turnover per year in the past 03 years (2015-16, 2016-17 and 2017-18) from their India Operations	Request Bank to revise turnover clause to 1000 Crores for atleast 2 of the last 3 years	No change in RFP terms

376	Annexure 8.2 - Pre-Qualification Criteria for Bidder	105	Point 6 - Customer reference	Bidder should have atleast 5 SIEM implemented /under-implementation in BFSI sector with atleast 1 implementation in regulatory and Public Sector Bank. Moreover, request bank to accept self-declaration from Bidder as due to NDA with Public Sector Undertakings, bidder might not be able to disclose customer name or furnish any document which can identify the customer (including PO copies)	No change in RFP terms
377	Annexure 8.2 - Pre-Qualification Criteria for Bidder	105	Point 7 - Customer reference	Request bank to accept self-declaration from Bidder as due to NDA with Public Sector Undertakings, bidder might not be able to disclose customer name or furnish any document which can identify the customer (including PO copies)	No change in RFP terms
378	Annexure 8.2 - Pre-Qualification Criteria for Bidder	106	Point 8 - Resources	Request bank to consider bidders with atleast 15 resource count, who have CISSP / CISA / CISM / CEH / ISO 27001 LA / LI certified	No change in RFP terms
379	Annexure 8.2 - Pre-Qualification Criteria for Bidder	107	Point 12 - Existing relationship	Request bank to include existing Security solution implementing/managing organizations	No change in RFP terms
380	Section 4.10	57	Implementation Timelines	Request Bank to modify timelines for delivery as stated below: - Submission of Detailed plan : 6 weeks from Acceptance of PO - Delivery of HW/SW - 9 Weeks from date of PO - Implementation & Commissioning - 16 Weeks - SIEM Integration - 20 Weeks - UAT - 24 Weeks	Refer to Corrigendum - 2
381	Section 7.1 -. Liquidated damages for delay in Delivery and Installation of Hardware and Software	95	7.1 b)	Request Bank to revise the LD for delayed deliveries to 0.1%/week with a cap at 1%	No change in RFP terms
382	Section 7.3 - SLAs & Liquidity Damages for CSOC Operations	98	Point 1	Request bank to revise response timelines as: Critical Events - 30 Mins High Priority - 45 Mins Medium & Low priority events - 60 Mins And Resolution times as: Critical Events - 4 Hrs High Priority - 8 Hrs Medium & Low priority events - 16 Hrs	No change in RFP terms
383	4.1 - SIEM	39		Please share Architecture details of SIEM, PIM, F/W Analyzer, APT. Do you required HA at DC & standalone at DR?	Please refer section 4 Scope of Work.
384	4	38		For PIM, NAC required at DR at "Rediness level". Please clarify Rediness at DR - our understanding is that customer requires Passive instance at DR. Please confirm.	The interpretation appears to be correct. Please refer section 4 Scope of Work.
385	4.1	39	Bank will supply only the Rack space, power and a network point in the Server room.	Hope bank will provide necessary racks also for placing the devices.pls confirm.	Yes. Bank will provide necessary rack space at DC, Mumbai and DR Site, Chennai.
386	4.1	40	C. Log collection	Need clarity from SIDBI where and all log collector required. Is it only at DC and DR ? Hope remote locations can push logs to DC thorugh SIDBI existing network. Please confirm.	The log collection devices are required at DC and DR. Please refer section 4 Scope of Work.
387	4.1	42	h) Notifications - The Notification Matrix defines the Bank's contacts, the incident management process step (initial, diagnose, update and resolve), the method (telephone, mobile, SMS, email) and hours (business hours or after hours). The Notification Matrix shall be customizable as per configuration item.	Hope Bank has SMS gateway . Please confirm.	The proposed solution should have required feature. The details will be shared with selected bidder. Please refer section 4 Scope of Work.
388	5.2	60	e) Score for the demo and presentation	Would request SIDBI to elaborate about demo and exact scope of Demo	The bidder is expected to give a demo of proposed solution as part of evaluation mentioned under Section 5.2 Technical Evaluation of the RFP.
389	11	143	Initial EPS requirement is for 5000. However, the appliance should be scalable up to 10000 EPS and the same appliance should support minimum 20,000 EPS	This compliance requirement says that 20000 EPS need to be supported but everywhere else it is 10000 EPS maximum. Please clarify this.	The bidder has to provide SIEM license for 10000 EPS from day 1 and same appliance should support/scalable upto 20000 EPS.
390	4.1	39	k) The bidder should provide SIEM license for 10000 EPS from day 1.	Many places RFP says that 5000 EPS is day 1 requirement. This is conflicting. What exactly be quoted 5000 EPS or 10000 EPS ?	The bidder has to provide SIEM license for 10000 EPS from day 1.

391	7.3	98	24x7 monitoring and reporting of all in-scope devices	As per Section 4.8.6, The bidder should monitor CSOC activities and events from each solution and devices already present in the bank's environment on a 12*6 basis (8 am to 8 pm) basis and suggest/ take appropriate action on an on-going basis. Is bank looking for 12*6 Monitorring or 24*7, please confirm the same.	The Bank is looking for 12*6 monitoring. The bidder has to maintain SLAs as per section 7 of the RFP.
392	3.2. Objective	32	Provide proactive threat intelligence and threat hunting.	Is the threat hunting service required throughout the contract period or is it periodical? If periodical then, please specify the frequency	Throughout the contract period on quarterly basis. Please refer section 4 of the RFP.
393	3.2. Objective	32	f) Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions on quarterly basis / as and when required by the Bank and provide solution for closure.	Can this be provided as a service form bidder's premises?	The Vulnerability Assessment is part of services but to be executed from Bank's environment.
394	3.2. Objective	32	j) Provide forensics support as per the requirement of Bank in case of any incident or as and when required.	Please specify the number of incidents per year for which forensics is needed	The support in forensics should be irrespective of numbers, the support in forensics will be required in case of incident, as and when required.
395	3.3 Current Information Technology Setup	33	• Further, three service providers are contracted to build the network. The bandwidth at the locations varies from 256Kbps to 32Mbps and at aggregation points (DC and DR) the bandwidth available is 4/32/64Mbps. Bandwidth at the locations is upgraded based on business requirements.	How many locations are on VSAT or non-MPLS connectivity? Please let us know the number of endpoints at these locations	The details will be shared with the selected bidder. Please refer to section 3.3 and Annexure 11.7 of the RFP
396	g. Internet	34	Web Gateway Security (WGS) appliance is installed at Data center and DR Site which acts as proxy server with content filtering, antimalware and antivirus software loaded on it. The WGS is integrated with AD.	Which is the current WSG being used? How many Internet gateways are currently present at SIDBI? Do all users have Internet access?	The details will be shared with the selected bidder. Please refer to section 3.3 of the RFP
397	g. Internet	35	Network Intrusion Prevention System (NIPS) is implemented at the perimeter and Antivirus software is implemented on all servers.	Please let us know the make of Firewalls, NIPS and AV being used currently	The details will be shared with the selected bidder. Please refer to section 3.3 of the RFP
398	4.1. Security Information and Event Management	38	d) Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.	Can the bidder propose for cloud based home grown ITSM tool or is it mandatory to propose on-premise COTS based ticketing tool	On-premises Incident Management tool is required.
399	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have breach detection rate of more than 99% as per NSS lab Breach Detection Systems test report & the test report should be submitted	Considering latest cyber security trends & breaches, Requesting bank to emphasis on Breach Prevention rather than detection only. Requesting Bank to consider NSS BPS Breach Prevention system test report with Block rate of 99% & above as per latest NSS BPS Report.	No change in RFP terms
400	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and/or other objects without relying upon any external box solution like Firewall / NGFW/ IPS/NGIPS/Web Proxy	Threats/IOC detected by Anti-APT & relevent intelligence should be shared across all security solutions including NGFW/NIPS for end-to-end protections at their level. Requesting bank revise clause to build shared intelligence architecture by integrating Anti-APT with NGFW.	No change in RFP terms
401	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed Solution should have throughput of 2 GBPS, have the ability to support both inline and out-of-band detection and should cause limited interruption to the current network environment. The Bank reserves the option of using deployment as Inline or out-of-band.	Anti-APT solution performance is also depend on no. of files emulated per hour/day/month as undersize appliance can add latency in network. Need additional appliance sizing information such as no. of emails/internet users & total no. of emails with attachment received per day/month, similarly total no. of files download happens through proxy per day/month. This data will help to size right appliance considering the user & file emulation capacity of device.	The average number of mails sent and received for one month: Sent - 12,000 Received - 60,000
402	Annexure 11.3 Anti – Advanced Persistent Threat	158	The proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack and the history of the movement of the malware in the network.	Kindly confirm if bank is also looking for Endpoint EDR agent solution for worksstations as part of this RFP. If Yes kindly share total no. of endpoints as well as OS flavours to consider.	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
403	Annexure 11.3 Anti – Advanced Persistent Threat / Performance	159	Solution should have a provision of 10G interfaces on Appliance proposed for Data ports.	Kindly confirm the no. of 10 GE interfaces to be considered?	10G interface is not required currently. However the proposed solution should have provision of 10G interfaces on Appliance proposed for Data ports.

404	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed solution should have capability of horizontal scalability.	Bank should consider Anti-APT in HA pair per site DC/DR which will protect bank network & traffic will not be allowed without inspection even in case of device failure.	No change in RFP terms
405	Annexure 11.3 Anti – Advanced Persistent Threat	159	The proposed Solution should be address HTTP,HTTPS,SMTP,SMTP CIFS, FTP and other protocols	Requesting bank to add on-box SSL inspection support to prevent threats coming through SSL or polymorphic channel. Requesting Bank to add specification as "Proposd Soluton should support on-box SSL inspection feature to prevent attack originating from SSL & Polymorphic Channel."	No change in RFP terms
406	Annexure 11.3 Anti – Advanced Persistent Threat/Endpoint Detection and Response	160	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp	Requesting bank to delete support for .chm & .com file-type as it's avoiding renowed vendor to participate. Kindly confirm if it is acceptable to be added as future enhancement.	No change in RFP terms
407	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Bank has asked for Multi-layer security methodolgy which includes Anti-Virus & Anti-bot along with Sandboxing. MAC & linux based malwares can be detected through windows platform based APT using multi-inspect engine & threat intel from cloud. Requesting bank to allow only Windows platforms & not both which disallows renowed vendor from RFP participation.	No change in RFP terms
408	Annexure 11.3 Anti – Advanced Persistent Threat	160	The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non-windows platforms and have capabilities to detect Mac, Linux and mobile malwares	Mobile malware come as .apk file & requires mobile specific ennviornment to emulate it. Kindly confirm if Bank is looking for separate Mobile solution as part of Mobile Security in this RFP? If Yes, Kindly share the total no. of Mobile devices to be considered?	There is no separate requirement for mobile security solution. However, the solution should support monitoring of mobile malwares for the connection originating from the mobile devices.
409	Annexure 11.3 Anti – Advanced Persistent Threat	161	The proposed solution should Block and hold file from spreading across all endpoints i.e. prevent lateral movement	We recommend bank to consider Endpoint EDR agent solution as part of this RFP which will protect lateral movements irrespective of Endpoint location such as online or offline (Roaming Laptops).	The endpoint agent is not required. The proposed solution should have mentioned capability if the bank requires in feature. Please refer Section 4 Scope of Work of RFP.
410	Annexure 11.3 Anti – Advanced Persistent Threat/Management & Reporting	161	The solution should support CLI, and must be administered through a web based console using SSH/HTTPS. Should support AAA for role based administration	Considering the huge CVE list of Browser exploits & vulnerabilities getting discovered every year. Requesting Bank to consider agent based console as more secure & fastest configuration mode. Requesting to add software console based configuration mode as well. Requesting Bank to revised clause as "The solution should support CLI, and must be administered through a web based/agent based console using SSH/HTTPS. Should support AAA for role based administration.	No change in RFP terms
411	4.1 - A -d	38	Inbuilt incident management and ticketing tool to generate tickets for the alert events generated by the SIEM or Separate tool which have capabilities of seamless integration. The tool should have feature to populate the relevant incident details from the alerts into the ticketing tool.	Please confirm if you have any existing ticketing tool or can we integrate it with our ITSM tool?	The proposed SIEM solution should have either inbuilt Incident Management tools or can be integrated with Incident Management tool to be provided by the bidder.
412	4.1- G	41	G. Incident management tool c) Solution should provide complete life cycle management (work flow) of trouble tickets from incident generation till closure of the incident.	As per this, will bidder be responsible for identifying the incident untill closure? Who will be closing the incident if there is a dependency from the bank side? This should not be ownership to the bidder.	The bidder has to propose Incident Management tool to identify the incidents generated from SIEM. The closure of the incident lies with the bidder however Bank will provide necessary support during the closure.
413	Annexure 11.3 - Anti-APT	158	The proposed solution should have breach detection rate of more than 99% as per NSS lab Breach Detection Systems test report & the test report should be submitted	NSS lab is just one of the validating agencies, also rating on the basis of catch rates,percentage of evasion detection etc for known attacks/ malwares is more relevent from an A/V perspective. Please clarify on this point.	No change in RFP terms
414	Annexure 11.3 - Anti-APT	158	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy environment.	XFF has to be supported on the proxy side to retain the original host IP address. Please clarify	The proposed should support the XFF forwarded messages for retaining the original IP address.

415	Annexure 11.3 - Anti-APT	158	The proposed solution should be deployed to protect Bank's IT Infrastructure from threat originating/coming from E- mail and Web.	Please share sizing parameters for E-mail around, clean emails per hour and attachments per hour.	The average number of mails sent and received for one month: Sent - 12,000 Received - 60,000
416	Annexure 11.3 - Anti-APT	158	The proposed Solution should be address HTTP,HTTPS,SMTP,SMTP CIFS, FTP and other protocols	Please clarify on why CIFS support is required for Web/Email vectors.	The proposed solution should have capability if the bank requires in future.
417	Annexure 11.3 - Anti-APT	158	The proposed solution should be able to provide customizable sandbox to match customer's endpoint environments, Sandbox must supports multiple operating systems for both 32-bits and 64-bits OS, Should Support multiple version of Windows and must have the ability to simulate the entire threat behavior	Please clarify on wheter the expectation is to have a sandbox for endpoint too as this point features under Endpoint Detection and Response. Also this point contradits ask in point 42 for customizable sandboxing.	The endpoint agent feature is not required, however the web and email appliance should support the feature. Please refer Section 4 Scope of Work of RFP.
418	Annexure 11.3 - Anti-APT	158	The proposed solution should have provision to identify entry point of malware.	Please clarify if the reference to entry point is to the parent process or the vector.	The proposed solution should able to identify the both parent process and initial attack vector.
419	Annexure 11.3 - Anti-APT	158	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.	Please clarify if this is for Email based detection or network based detection	Both the appliance should have the required capability.
420	Annexure 11.3 - Anti-APT	158	The proposed solution should have usable storage of 2 TB and support at least 6 Ethernet Interfaces	Please clarify if this is for Email based detection or network based detection	2TB storage on the proposed appliance of solution is to capture all logs/files and additional ports may be required for scalability in the future. The same applies to both the APT appliances.
421	Annexure 11.3 - Anti-APT	158	The Proposed solution for Email Anti-APT should be deployable in inline mode as MTA.	Please provide sizing and architecture details.	The average number of mails sent and received for one month: Sent - 12,000 Received - 60,000
422	Annexure 11.3 - Anti-APT	158	The proposed solution shall support Local Password & Radius for authentication schemes	Radius is a traditional methodology of authentication. Request that this point be modified to include 'or support priviledged Identity management software for authentication shemes.	The proposed solution should support local, radius and PIM authentication.
423				Wanted to know if there is any EMD exemption if we are MSME certified (Certificate attached).	Please refer to Section 6.54 added as part of Corrigendum
424	Annexure 8.2 Point 12	107	The Bidder should not be existing Service provider providing services for Network Management (NOC) / Facility Management / Data Centre Services / Data Centre Management for SIDBI to avoid conflict of interest.	Request you to relax the clause.	No Change in RFP terms
425				Please provide the number of Privileged users for which you need to factor the PIM solution.	The number of privileged users to be integrated with PIM solution are 70.
426	Annexure 8.2 Pre-Qualification Criteria for Bidder	107	The Bidder should not be existing Service provider providing services for Network Management (NOC) / Facility Management / Data Centre Services / Data Centre Management for SIDBI to avoid conflict of interest.	Please explain scope of existing service provider of NOC to SIDBI.	The bidder should not be an existing service provider, providing any administrative, monitoring and managing services for any servers / databases / network devices (either owned by SIDBI or managed by third party for SIDBI) of SIDBI to avoid conflict of interest.
427				We request you to consider "Global reference (outside India) and non-BFSI industries also" for the following qualification criteria, that will allow us to participate in the RFP. Request you to please consider. 	No change in RFP terms.
428	Annexure 8.2 Pre-Qualification Criteria for Bidder		The bidder must have implemented / under implementation of security operation center / Cyber security operations center in at least 2 BFSI customers in India having project cost 5 Cr and above.	The project cost for the implementations should be as below : 1. One project cost should be 15 crores and above 2. One project cost of 5 crore and above 	No Change in RFP terms
429	VAPT			Saw you have mentioned you are locking PT also with propose solution but sir there is no VA tool who provide the PT also because not match the standard practice. Please suggest if you are ok with cloud base solution. Request you to kindly help with below details for further process.	No Change in RFP terms

430	Section 4.8.5	52	System Integration Testing (SIT) and User Acceptance Testing (UAT)	Is bank having dedicated UAT/Test environment for Network prospective? Is bank will retain UAT/Test setup throughout the contract year or it will dissmental after successfully testing of UAT?	There is no dedicated test environment available for network perspective. The bank will not retain the UAT / Test setup after successful testing of UAT. However, all the updates/patches/fixes need to be tested in UAT before pushing these to production environment.
431	Section 4.8.1	47	There should be three separate environments: Development, Test (UAT), and Production (DC-DR). The environments must be configured on a separate physical servers. The Development environment should have at least 20% and Test (UAT) environments should have at least 50% of the configuration of the Production environment quoted by the Bidder	20% licences for Dev and 50% for UAT will be an overkill. Dev & UAT environment will only be used for testing new polices/config, modification of policies/config, upgrade/updates	No Change in RFP terms.
432	Section 4.10	56	i. NAC: Integration of NAC on around 100 end user devices. ii. PIM: Integration of 50 servers (all privilege users) with PIM iii. Firewall Analyzer: Integration of 10 firewalls with Firewall Analyzer iv. Anti-APT: Integration of web proxy server and email server with Anti-APT	It's recommended to have max 10 End user devices for UAT/tesing of security tools. In order to create Dev & UAT, we would also need 20% additional endpoints for Dev and 50% additional endpoints for UAT for creating the setup. Does SIDBI have these number of endpoints to be allocated for Dev and UAT? In addition to endpoints, switching ports will also be needed. Appropriate Network setup will also have to be created for Dev & UAT of Network technologies such as APT.	No Change in RFP terms. Additional endpoints for Dev & UAT are not required. Please refer to Annexure 11.7 of the RFP. However, all the updates/patches/fixes need to be tested in UAT before pushing these to production environment.
433				Timelines for implementation / completion to be increased to 24 weeks.	Refer to Corrigendum - 2
434				Please extend the project implementation timelines to 24 weeks post acceptance of PO.	Refer to Corrigendum - 2