S. No.	Section Name	Page No.	Point as stated in RFP	Description	SIDBI Response
1	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	As per RFP total 10 Firewalls we need to integrate with Firewall Analyzer, requesting bank to share all 10 firewalls is in cluster pair (Active-Passive) or standalone firewall. This will help us to rightly size Firewall analyzer solution. Getting total count of L3 routers/switches in the pre-bid query as it is important to build the network topology for change management to work automatically, so requesting bank to share count of L3 router/switches.	Bank currently has 5 cluster (10 firewalls) in active -active mode and one standalone firewall. Please Refer to Point No. 7 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
2	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	Adding APT integration with firewall/NIPS, it will help bank to bank create a more stable architecture. Anti-APT will focus to detect majorly on unknown threats/IOC & Firewall/NIPS which are inline & capable of blocking known malicious traffic.	Please refer to Point No. 400 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
3	Section 4.3	42	General Query	is it ok to configure Web & Email APT solution on single appliance?	This should be configured on separate appliance to avoid single point of failure.
4	Section 4.8.5	52	System Integration Testing (SIT) and User Acceptance Testing (UAT)	If bank will not retain UAT environment, then how bidder will test new patches / updates / fixes in UAT environment before production?	Please refer to Point No. 430 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
5	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.	We understand that a packet capture solution needs to factored for this requirement, for sizing the packet capture solution across DC & DR we need below info. 1> No of Ports required for DC & DR 2> Breakup for 10Gbps throughout across DC & DR 3> Retention Policy i.e (Raw packet & Meta data) - Do we need to capture the packet for LAN & Internet segment	Throughput for internet traffic currently at DC is 64*2 MBps and 32*2 MBps at DR. Packet capture solution should support 4 network ports (2 X 1 Gbps + 2 X 10 Gbps) and store Raw Packet for 7 days and Meta data for 30 days.
6	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.	The data/logs required should be made available for the solutions deployed by the bidder/OEM.
7	Annexure 11.5 Network Access Control (NAC)	167	The solution should support alerting mechanism such as e-mail, SMS etc.	Please modify this clause to, The solution should support alerting mechanism such as e-mail/SMS by integrating with the Sylog and SIEM solutions.	Please refer to Point No. 181 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
8	Annexure 11.5 Network Access Control (NAC)	167	The solution should permit admin to define thresholds for threat levels received from the NAC	Our understanding is that the NAC should do a posture check and set basleine policies thresholds. E.g check antivirus patch is available on endpoint	The interpretation appears to be correct.
9	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.	Our understanding is that the NAC should do a scanning check on endpoint and set basleine policies. E.g check antivirus is available on endpoint if not block/remidiate the endpoint.	The interpretation appears to be correct.
10	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.	Business impact here defines impact on systems / applications existing in the network.
11	4.4. Firewall Analyzer	43	Integration of 10 firewalls with Firewall Analyzer	SIDBI has mentioned 10 Firewalls as the count for FA solution. Request bank to confirm if all these are in Cluster which means 5 Clusters/Pair Or 10 Clusters/Pair.	Bank currently has 5 cluster (10 firewalls) in active -active mode and one standalone firewall.
12	7.2. Liquidated damages for not maintaining uptime	RFP Page 95, Point # 7.2	a) The bidder shall guarantee 24x7 availability with monthly uptime of 99% for the all the solutions under this project during the period of the Contract.	To achieve 99% uptime all the solution needs to be considered in HA at DC & DR, request bank to confirm on the same accordingly.	No Change in RFP Terms. Please refer to Section 4 and Section 7 of RFP
13	Annexure 11.4 Firewall Analyzer	RFP Page No 163 Point no 11	The proposed solution should generate enterprise-wide interactive network map based on the routing information and topology of the added devices	Request bank to provide total L3 routers/switches counts, as it is important to build the network topology for change management to work automatically. We need the count of L3 routers/switches if any to avoid issues at the later stage.	Refer to Point No. 7 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019

14	Pg 47, 4.8.1. Hardware, Software and Network Connectivity		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 per this clasue, our understanding is that we need to consider additional license & appliance. Request bank to confirm if our understanding is per below is correct or not: 1) SIEM - For Dev, we need to factor additional 2000 EPS license with separate appliance. For UAT, we need to factor additional 5000 EPS license with separate appliance. 2) NAC - This is appliance based solution. For Dev, we need to factor additional 320 license with separate appliance. For UAT we need to factor, additional 800 license with separate appliance 3)APT- This is appliance based solution. For Dev, we need to factor additional appliance with capacity of 20% of production setup. For UAT, we need to factor additional appliance with capacity of 20% of production setup. This way we need to factor 3 appliance to appliance considered for production. 4)Firewall Analyzer - For Dev, we need to factor 20% additional license. For UAT we need to factor 50% additional license. We also need to consider separate hardware(server) for Dev & UAT. 5) PIM - For Dev, we need to factor 20% additional license. For UAT we need to factor 50% additional license. 6) VAPT services- For Dev, we need to factor 20% additional license. For UAT we need to factor 50% additional license	Please refer to Point No. 430 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
15	4.1. Security Information and Event Management A .Solution Implementation:		j)The bidder will be responsible for providing P2P linkfor the log replication collected by SIEM log collectorsacross primary DC site and DR site.	Request bank to share the address of DC & DR as this is required to share with Telecom service provider who in turn will do the feasibility and share the quote with us	The bank's data centre site is located at Mahape, Navi Mumbai and disaster recovery site is located at Siruseri, Chennai.
16	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
17	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.		Please refer to Corrigendum - 3
18	4.8.3.□mplementation & Integration> z	50	z)□EM 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.	We assume that back-to-back support requirement is related to bug-fixes, hardware mainetenance and OEM L4 support, however day-to-day operations management will be done by Bidder's L1/L2/L3 engineers. Please confirm.	The interpretation appears to be correct.
19	4.8.3.□mplementation & Integration	50	t> viii.□ecurity Patch management procedure	Patch management as stated here is limited to patching the software and hardware provided as part of CSOC by the bidder. While patch management for the existing IT infrastructure for other applications will be done by respective services partner or SIDBI infra team. Please confirm and suggest the expectation on the same.	Please refer Section 4 Scope of Work of the RFP.
20	4.8.3.□mplementation & Integration	51	gg)□SOC 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.	Please provide frequency & details of audits that happen in a fiscal year?	The details will be shared with selected bidder.
21	4.8.6.□onitoring	52	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.	For the underlying hardware solution (e.g. Server, storage, network switches, backup devices). Please suggest if bidder can leverage on existing infra monitoring tools for availability management. Incase existing tool can be leveraged please provide the details or confirm if bidder needs to include the same in BoM.	The bidder needs to propose infra monitoring tools for availability management and needs to be included as part of BoM.
22	4.8.6.□onitoring	52	General	Please suggest, if bidder can leverage existing patch management tool for patching the servers of the proposed CSOC infra. Please provide details of patching tools available with SIDBI for server patching?	The bidder needs to propose patch management tool for patching the servers of proposed CSOC infrastructure.

23	7.3 SLAs & Liquidity Damages for CSOC Operations	98	•24x7 monitoring and reporting of all in-scope devices	Monitoring and reporting service window is mentioned as 24X7, while the resource availability service window is 12*6 basis (8 am to 8 pm) as mentionedi n 4.8.6 Monitoring section on Pg. 52. Please confirm if the availability monitoring and reporting will be limited to auto-alert generation and auto-ticket logging using the tools, and how the penalty credits will be calculated in case where resources are not available in non-RE Shift.	The resource availability needs to be provided on 12*6 basis and monitoring and reporting service needs to be provided on 24*7 basis. The penalties / liquidated damages will be calculated as per the resource availability window defined in the RFP currently. If in future, bank requires resources on 24*7 basis the liquidated damages will be calculated as per the resource availability window.
24	7.3 SLAs & Liquidity Damages for CSOC Operations	98	Liquidated Damages	Please confirm if the penalty credits mentioned are attributable to individual incidents or are on cummulative number of incidents in a quarter, as no Target for SLA achievement is given (e.g. resolution as expected for 95% tickets in a Quarter)	Please refer to Corrigendum - 3
25	7.2 Liquidated damages for not maintaining uptime 7.3 SLAs & Liquidity Damages for CSOC Operations	98	Liquidated Damages: n)Hbowever, the maximum LD levied shall not be more than the 10% of total value of the order per quarter. n)Hbowever, the maximum LD levied shall not be more than the 10% of total value of the order per quarter.	Please confirm if there is any Penalty cap for the LDs mentioned for section 7.2 is applicable for the SLA credits mentioned in section 7.3 also. Or suggest what is the max penalty cap for the SLA credits mentioned in section 7.3	Please refer to Corrigendum - 3
26	7.2 Liquidated damages for not maintaining uptime	97	l)Eor 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.	Please cap the penalty to pro-rata daily payout of the individual resource as per the cost provided for resources to SIDBI.	Please refer to Section 7 of the RFP.
27	7.2 Liquidated damages for not maintaining uptime	97	k)Hn the case of failure of P2P Link, the proportionate cost of the no. of day's service not available will be deducted.	As per the scope document DC & DR link will be provided by SIDBI also, entire service delivery is expected from onsite, hence no connectivity to bidder's offshore SOC center. Please suggest which P2P link penalty credits are applicable here.	Refer to Corrigendum - 3
28	7.2 Liquidated damages for not maintaining uptime	97	k)Hn the case of failure of P2P Link, the proportionate cost of the no. of day's service not available will be deducted.	In case of DC & DR P2P link availability, same will be provided by SIDBI through a ISP. This penalty should be applicable to them as bidder will have no control on their services delivery and can only do vendor co-ordination for the quicker resolution.	Refer to Corrigendum - 3
29	7.3 SLAs & Liquidity Damages for CSOC Operations	98%	Point 1: Incident response Point 2: Incident resolution Point 3: Reports and Dashboard Point 4: Vulnerability Assessment Point 5: VAPT advisory & remediation services Point 9: Security Device Management and Administration	1. Suggestions: Critical - 5%, high priority - 3%, medium - 2% 2. Suggestions: Critical incidents within 120 minutes, High priority incidents within 120, Medium priority incidents within 180 minutes 3. Suggestions: No penalties on reports 9. : No penalties on VAPT reports For rest points: Suggestion: max penalty will be 3%	No Change in RFP Terms
30	7.3 SLAs & Liquidity Damages for CSOC Operations	98	Liquidated Damages	We suggest if SIDBI can cap the total SLA penalty credits to maximum 3% of the total quarterly Operations cost.	No Change in RFP terms
31	VAPT Information and Remidiation Services	44	Bidder should execute this service on quarterly basis	We recommend VA to be done quarterly and PT to be one every six months	Please refer to Section 4 of the RFP.
32	Other General Requirement	46	The bidder needs to propose only Veritas backup solution for backups	Would request bank to consider other backup solution as well	Please refer to Section 4 of the RFP.
33	Other General Requirement	46	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	Would request bank to provide more details about different setups	Please refer to Point No. 430 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
34	Implementation & Integration	50	In case a device goes down at DC, the operation and function being performed by the device should be taken over by a corresponding device at DR site and vice versa	As per the understanding, solutions in DC will be in standalone mode, we don't have to consider any high availability or failover mechanism at DC for any solution. Please confirm.	Please refer to Section 4 Scope of the work of RFP.
35	Implementation phases and Timelines	57	Delivery of CSOC Hardware / Software and licenses and resources	Would request bank to change it to 8 weeks from acceptance of PO for delivery	No Change in RFP Terms. Please refer to Corrigendum - 2 published on 15-03-2019
36	Implementation phases and Timelines	57	Deployment of CSOC Resources at Bank's premises	Would request bank to change it to 12 weeks from acceptance of PO	No Change in RFP Terms. Please refer to Corrigendum - 2 published on 15-03-2019
37	Implementation phases and Timelines	57	Installation & Configuration of SIEM and other Security Tools / Solutions	Would request bank to change it to 12 weeks from acceptance of PO	This has been changed to 10 weeks from acceptance of PO. Please refer to Corrigendum - 2 published on 15-03-2019
38	Implementation phases and Timelines	57	Integration of SIEM with other Security Tools / Solutions under CSOC	Would request bank to change it to 20 weeks from acceptance of PO	This has been changed to 14 weeks from acceptance of PO. Please refer to Corrigendum - 2 published on 15-03-2019
39	Implementation phases and Timelines	57	User Acceptance Test (UAT) and making the CSOC operational	Would request bank to change it to 23 weeks from acceptance of PO	This has been changed to 18 weeks from acceptance of PO. Please refer to Corrigendum - 2 published on 15-03-2019
40	Annexure 11.1 Security Information and Event Management	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	Is high availability of collector required in DC or this point discusses about single log collector at DC and single log collector at DR and both will work for failover of each other. Please confirm.	The proposed solution should have mentioned capability for high availability.

41	Scope of Work - Security Information and Event Management	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.	Technically log sources will send traffic to both DC and DR log collector simultaneously. What is the storage expected at DR and for how many days, logs should be kept at DR log collector. Please suggest.	Please refer Section 4 Scope of Work and Section 4.1B Storage of the RFP. The DC requirements will be as per section 4.1 B of the RFP. For DR, The SIEM should be able to maintain 3 months of logs on-box.
42	Scope of Work - Security Information and Event Management	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.	Reselling bandwidth requires SP license and only authorized service provider can do the same. Would request bank to povision P2P link on behalf of bidder.	Please refer to Corrigendum - 3
43	Scope of Work	37	At DR, Log collection device only	In case of DC going down, only log collection will happen at DR, Bank will not be able to perfrom any other activities (such as reporting, correlating etc.) will not be available till the time DC is down. Hope this behaviour is ok with bank. Please confirm.	Please refer to Section 4 Scope of the work of RFP.
44	3.2 Objective	32	Provide forensics support as per the requirement of Bank in case of any incident or as and when required	Please share the expectations on Forensic scope and what activities SIDBI expects partner to perform? Does SIDBI expect tool for forensic support? If yes, please share detailed expectations.	Please Refer to Point No. 312 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
45	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?	Please Refer to Point No. 6 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
46	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?	Please Refer to Point No. 7 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
47	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 to Point No. 356 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
48	SIEM		Packet capture solution	Packet capture solution is required at DC and DR both or only at DC.	Packet capture solution is required only at DC.
49	SIEM		Packet capture solution	It is recommended to capture packets from Internet. 10 Gbps throughput may not be required looking at SIDBI environment. Ideally, 500Mbps throughput with 15 days raw logs storage and 30 days meta data storage should be enough. Please consider the same and update packet capture sizing details	Throughput for internet traffic currently at DC is 64*2 MBps and 32*2 MBps at DR. Packet capture solution should support 4 network ports (2 X 1 Gbps + 2 X 10 Gbps) and store Raw Packet for 7 days and Meta for 30 days.
50	Annexure 11.3 Anti – Advanced Persistent Threat		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.	Expecting “history of the movement of the malware in the network.” To be deleted as it will ideally require NAC or EDR solution.	Please Refer to Point No. 251 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
51	Annexure 11.3 Anti – Advanced Persistent Threat		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	Requesting to remove “non-windows platform” & “Linux/Mobile Malwares”	No Change in RFP terms.
52			Advanced Persistent Threat	Bank has asked for separate WEB/Email APT in techincal BOM. Need clarification if bank need separate appliances for both vector or if one appliance can fulfil bank's requirement then bidder is ok to quote single appliance for both vectors, this will help bank to save cost	This should be configured on separate appliance to avoid single point of failure.
53			Firewall Analyser	Please mention number of firewalls in cluster and in standalone mode, this is required for sizing of the soution	Bank currently has 5 cluster (10 firewalls) in active -active mode and one standalone firewall.
54	5. Evaluation Methodology		5.1D. 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.	We recommend bank to include CEH and SIEM product certification also in the evaluation criteria and also reduce the count to maximum of 10, instead of 20	No Change in RFP terms
55	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	Please Refer to Point No. 240 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
56	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	Please Refer to Point No. 241 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
57	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.

58	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.	Please Refer to Point No. 246 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
59	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.	Please Refer to Point No. 277 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
60	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	Please Refer to Point No. 278 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
61	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.
62	7. Service Level Agreement & Liquidated Damages	100	All the above LDs are independent of each other and are applicable separately and concurrently.	Request Bank to clarify that the total LD including delivery, installation, SLA, Uptime and man power, is 10% of TCO.	Please refer to Corrigendum - 3
63	6.13. Terms of Payment and Payment Milestones	69	Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost) 50% on delivery 20% on UAT signoff 30% on Project signoff	Cost of Product including OEM warranty for 3 years (including CSOC Solution License, Hardware and Storage Cost, Other Software License Cost) 70% on delivery 20% on UAT signoff 10% on Project signoff	No Change in RFP Terms.
64		Page no 32	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	Are there applications in scope for Security Testing? Can you please share the number of applications? please share the required details below:-- No of Static Pages, No of Dynamic pages, No of URLS	Application Security testing is not part of scope. Please refer section 4 Scope of Work of RFP.
65		Page no 2	Security Testing	The expected frequency of conducting Application Testing ?	Application Security testing is not part of scope. Please refer section 4 Scope of Work of RFP.
66				We appreciate the extension in submitting the bid till 28th March. However, we would require a 2 week further extension in submitting a quality response (also keeping year end activities in mind) and thus request the submission be extended till 11th April.	Please refer to Corrigendum - 3
67				We need further clarification on few points which are critical because these were not responded by bank in corrigendum. On these points we need more clarity to design appropriate solution. Also in the wake of these gap and year end we require more time for submitting the bid. Kindly accord approval to extend this till 12th of April'2019.	Please refer to Corrigendum - 3
68	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.	Request Bank to remove word Packet Capture as there is no mention of packet capture in commercial format.	No Change in RFP terms
69	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 per section 4 SOW, bank never mentioned about SIEM architecture. Is it standalone/HA required for SIEM in DC-DR. To be everybody on same page, please share SIEM architecture requirement at DC-DR. As per standard, SIEM is having 3 layer (Collection, Logger (storage), Correlation). Please let us know bank required all 3 layer standalone in DC & DR or all 3 layers HA in DC and in DR.	The proposed solution should have mentioned capability for high availability.

70	4.1. Security Information and Event Management A. Solution Implementation:	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	Please share sample SIEM architecture requirement at DC-DR. If Logs are to be replicated between DC and DR then there will be a logger or storage required in DC & in DR. since this is affecting cost pls give clarifications on architecture.	Please refer Section 4 Scope of Work of the RFP.
71	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.	Please share below detail to rightly size Email APT solution: 1) Total number of clean email (after anti-spam) per month (current) & growth per month requirement. 2) Total No. of Mailboxes. 3) whether its Microsoft Exchange online or is it hosted with a third party service provider.	1. The total number of clean email sent / received per month on an average is approximately 14,000. 2. The total number of mailboxes are approximately 1600. 3. All the mailboxes are hosted in Microsoft Exchange Online.
72	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.	Clarification on Pre-Qualification Criteria for Bidder : One of the NOC providers have asked on the scope of services as part of NOC that will qualify as conflict of interest.	Please refer to Point No. 426 as part of "CSOC Pre Bid Queries Response" published on 15-03-2019
73	Annexure 8.10		Pre-Contract Integrity Pact	Integrity Pact - The document is still the same, as per CVC guidelines the new document is available	No Change in RFP terms
74	Section 7			We had requested the bank to kindly acknowledge our understanding that capping of Penalty and LD together at 10 % of total contract value each year	Refer to Corrigendum - 3
75				Bank has asked to submit cost of RFP(Rs 5000) in the form of DD payable at Chennai. As per corrigendum 2, bid submission is in SIDBI BKC office. Kind request to confirm if we need to submit DD payable at Chennai or Mumbai considering the change in place of bid submission.	The DD needs to be payable at Mumbai.
76			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.	Software based solutions are highly scalable and can be scaled horizontally. As SIDBI has asked for log collection from various geographical locations; with this requirement software based solutions are very flexible and can be deployed anywhere when required. This was clarified during pre-bid meeting that proposed solution can be deployed on hardware supplied by bidder but in the query response it is mentioned that solution should be appliance based. We request bank to please let us know if proposed solution can be software based deployed on hardened operating system/appliance based solution.	No Change in RFP terms
77			The SI should prepare a DR plan for switch over in case the DC operations are down	In Section 4 of SOW; SIDBI has asked only log collection module in DC & DR and SIEM only in DC. Page number 39 SIDBI has asked for automated online replication of logs between DC & DR. Log replication means availability of logs in DR. Please let us know what exactly SIDBI is looking for. SIEM in DC only in standalone mode with log collection from DR also or SIEM in standalone in DC & standalone DR along with log collection in DC & in DR?	Please refer Section 4 Scope of Work of the RFP.
78			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.	We would like to know if SIDBI is looking for site level redundancy also SIDBI has mentioned that there are multiple geographic locations. We would like to know if SIDBI is looking for software based solution to collect logs from all locations as this will be easy to deploy anywhere even in cloud public or private cloud platforms. Please confirm.	No Change in RFP terms