Response to Pre-bid Queries

REQUEST FOR PROPOSAL (RFP) FOR

Selection of Service Provider for Cyber Security Operation Center on Hybrid Model

RFP No.: PDCC/IT-Tender/2024-25/002

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
1	Tender Fee (non-refundable) by Demand Draft/ Banker Cheque only	6	1.2	Tender Fee (non-refundable) by Demand Draft/ Banker Cheque only INR 15,000/- + INR 2,700/- (GST) = INR 17,700/- (Seventeen Thousand Seven Hundred Rupees Only) favoring 'The Pune District Central Co-operative Bank Ltd.'	Request PDCC to please confirm whether we need to re-submit Tender fee, or if the previously submitted DD will be considered?	Tender fee to be resubmitted as it's a new Tender.
2	1.2	7	Request for Proposal	Last Date, Time and Place for submission of Bid 02.09.2024, upto 15:00 hours The Pune District Central Co-operative Bank, IT Dept. Head Office: 4 B, B. J. Road, Pune - 411 001.	Please extend the submission date to 16th September	Revised Clause: Last Date, Time and Place for submission of Bid 10.09.2024, upto 15:00 hours The Pune District Central Co-operative Bank, IT Dept. Head Office: 4 B, B. J. Road, Pune - 411 001.
3	2	9	Detailed Scope of Work	Network Access Control (NAC)	As you required On-Prem NAC Solution, can you confirm 1) How many End Point need to be consider. 2) Are all Branch Location Directly connected to DC-DR 3) Whether all the End Point are on-boarded on Active Directory 4) Any Specific Posture Check Requirement 5) At branch level all switch are L3 or L2 & what are the Make & Model	1) Kindly Refer Point No 2. Detail Scope of Work 2) Yes, all Branch Location Directly connected to DC-DR 3) Understanding is correct. 4) To be discussed with selected bidder during implementation 5) All branches having L2 switches of Cisco make.
4	2	9	Detailed Scope of Work	Endpoint Detection and Response (EDR)	What is the Current Anti-Virus Solution	TrendMicro

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
5	2	9	Detailed Scope of Work	Network Behavior Anomaly Detection (NBAD	As per TCL SIEM/SOC Solution NBAD is integrated Solution. Is there any Specific required to go with On-prem dedicated Solution for NBAD	NBAD should be on-premises as mentioned in RFP.
6	2	9	Detailed Scope of Work	Database Activity Monitoring (DAM)	In Inventory List you have mention 5 DB isn DC & 5 in DR, So you required dedicated DAM Solution or Only DB Audit Log can be integrated with DB to monitor the threat	Please refer RFP requirement.
7	2	9	Detailed Scope of Work	Privileged identity and Access management (PIM/PAM),	How many user access required to PIM/PAM Solution	Kindly Refer Point No 2. Detail Scope of Work
8	2	9	Detailed Scope of Work	External Firewall with NIPS	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
9				Core Next Generation Firewall with NIPS, Analyzer	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
10				Endpoint Security with Anti-Virus and HIPS	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
11				Data Loss Prevention	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
12				Anti-DDoS solution	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
13				Enterprise Management Solution	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
14				Patch Management	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
15				VPN	Required Make & Model	Sophos
16				Email solution along with Security	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
17				SSL VPN	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
18				SSL Interceptor	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
19				Load Balancer	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
20				WAF	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
21				Anti- Advanced Persistent Threat (Anti-APT) (Through External Firewall)	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
22				Backup tool	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
23				Sandbox	Required Make & Model	Kindly Refer Point No 2. Detail Scope of Work
24				Proxy Server	Required Make & Model	CC Proxy
25				AAA, TACACS Server	Required Make & Model	Cisco iSE
26	2. Detailed Scope of Work	9		The bidder is expected to provide the below mentioned services and ensure 24*7*365 coverage for all devices and instances at the Data Center, DR Site, NDR, HO, Branches and Service Outlets and for the hardware/software applications of the PDCC Bank. Bank expects below solutions to be provided as part of SOC, but the management & monitoring will cover all devices & solutions implemented at bank's end.	Request for Clarification : In Part 1 Bank is asking for, *"The bidder is expected to provide the below-mentioned services and ensure 24*7*365 coverage for all devices and instances at the Data Center, DR Site, NDR, HO, Branches and Service Outlets and for the hardware/software applications of the PDCC Bank."* Our Understanding: Yes, the requested security solution with 24/7 security incidents monitoring will help the Bank's IT infrastructure to protect from cyber security attacks and have better security posture visibility once the tools and monitoring services are fully operational. But at the same time, we assume Bank must have Device Management and a dedicated FMS Team with AMC support for the Data Center, DR Site, NDR, HO, Branches and Service Outlets and for the hardware/software applications of the	24*7*365 Monitoring of the proposed Hardware, applications and services should be provided by bidder.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					PDCC Bank, and the same is bidders Out-of Scope in this "Cyber Security Operation Center" RFP	
27	2. Detailed Scope of Work	9		Endpoint Forensic and Behavior Analysis (EFBA)	WRT to behavior analysis, is PDCC looking for a solution like UEBA apart from with forensics? Apart from incident investigations, What other use cases require forensics? Current Volumes: How many incidents are reported per month that require forensic analysis?	It will be shared with Final selected bidder.
28	2. Detailed Scope of Work	9		Endpoint Forensic and Behavior Analysis (EFBA)	Request for Clarification: Please confirm if our understanding is correct bank has already asked for 50 Hours per Year Cost for Forensic Support in Annexure 11 Commercial Bill of Material under FM Services.	Understanding is correct
29	2. Detailed Scope of Work	10	Bank's s expected hybrid deployment strategy of the proposed solution is as mentioned below:	Network Behavior Anomaly Detection (NBAD) listed proposed under Solution Deployment On - Premises	We Request you to kindly amend it to Solution Deployment via Managed SOC as this solution needs to be integrated with the part of SIEM solution that will be taken care by Managed SOC	RFP Requirement Stands
30	2. Detailed Scope of Work	11	7	7. Bidder shall provide SIEM solution, which can monitor below mentioned Assets to be integrated for SOC and in addition the solutions being provided by bidder as part of CSOC.	Request for clarification: Here Bank is willing to procure the SIEM solution licenses in their name and implementation and management by the bidder or wants the complete solution as a services model ?	SIEM will be on services model.
31	2	11	5	Delivery of CSOC Hardware/ Software and licenses and resources	Request Bank to change the hardware delivery timeline to 10-12 weeks, as if will not be possible to deliver hardware in 6 weeks	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
32	2	11	5	Delivery of CSOC Hardware/ Software and licenses and resources	Request Bank to include the implementation period for the infra also as that is missing the timeline, Hardware/infra implementation should be considered for 4 Weeks	Kindly refer RFP clause: "Time Schedule of the Project" point no. 6: Installation & Configuration of SIEM including HA and DC-DR -NDR setup. NDR will not have any CSOC components implemented but NDR's devices shall be monitored through CSOC.
33	2.1	12	The Bidder is expected to do following but not limited to:	Point 1 The bidder is expected to provide 4 (Three (3) L1 resources and One (1) L2 resource) members team (For L2, will work during office hours and For L1, will work 24*7*365 in shifts. Resources should be available during Bank holidays)	Bank to clarify if the resources needs to be working on all Bank Holidays & Weekends for only in case of emergencies. How does the bank plan to give mandatory holidays to the resources as per Labor Law.	Kindly Refer RFP Clause: 2. Detailed Scope of Work
34	2.1	12	The Bidder is expected to do following but not limited to:	Point 7. Bidder shall provide SIEM solution, which can monitor below mentioned Assets to be integrated for SOC and in addition the solutions being provided by bidder as part of CSOC. Any new solution (SD-WAN, Micro-ATM & Future solutions) procured during the tenure of the project to be added as part of monitoring.	Any new addition of log sources will be treated as scope beyond what is mentioned in the RFP and commercials for the same will be discussed mutually.	RFP Requirement Stands
35	2.1	12	The Bidder is expected to do following but not limited to	Point 8. The SIEM tool should be capable of sending automated email and SMS as other modes of communication for alerts related to critical incidents.	Requesting to add "or" in the clause: The SIEM tool should be capable of sending automated email and / or SMS as other modes of communication for alerts related to critical incidents.	RFP Requirement Stands
36	2.1	12	Point 7	Bidder shall provide SIEM solution, which can monitor below mentioned Assets to be integrated for SOC and in addition the solutions being provided by bidder as part of CSOC. Any new solution (SD-WAN, Micro-ATM & Future solutions) procured during the tenure	Can you clarity that In future in new inventory is on-boarded on CSOC, Then this additional services will be as per the rate card provided by service provider	Kindly Refer RFP Clause: 2. Detailed Scope of Work

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				of the project to be added as part of monitoring.		
37	2. Detailed Scope of Work	12	9	9. Log has to be retained for a period of 6 months Online and additional 6 months offline. SIEM should collect log from all solutions mentioned in table of point no 7. and provide a comprehensive picture. If bank procures any additional devices /solutions/Services during the tenure of contract the same should be integrated in SIEM free of cost.	Request for clarification: Please confirm if our understanding is correct: the log management solution software with sizing details will be provided by the bidder and the required server and storage will be provided by Bank.	Required server & storage to be provided by bidder as mentioned Sow
38	2. Detailed Scope of Work	12	17	17. Providing adequate resources for Cyber Security Operations Centre (C-SOC) and should continuously coordinate with the onsite team.	Request for clarification: As the RFP states Cyber Security Operation Center on Hybrid Model, Dose the Bidder need to provision dedicated resources for for Bank sitting in Bidder CSOC (Remote SOC). We suggest to go for Shared CSOC resources this will be much more effective and will helpful in optimizing the overall resources cost.	Kindly refer RFP point no. 2.2 Onsite Resource Experience, CSOC Monitoring should be done by shared resources at Bidder's Cyber SOC and 4 dedicated resources should be deployed at Bank site for required co-ordination & configuration, Monitoring, Management & support of solutions deployed at Bank's DC, DR & NDR. NDR will not have any CSOC components implemented but NDR's devices shall be monitored through CSOC.
39	2.1	12	3	Procurement of the necessary solutions and the corresponding hardware, software, database etc. required for implementing these solutions. Bank will provide the required space & power to implement these solution on DC, DR & NDR for optimum uptime. Any network & power cables needed to integrate the solution with Banks existing architecture is to be arranged by	What is the expected power input provided per rack, need to sizing the rack accordingly based on the power consumptions	6-7 KVA/Rack Max.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				bidder. All solutions to be in HA mode in DC & standalone mode in DR/NDR		
40	RFP No.	12			suggested uptime penalty to be reduced to 95%	RFP requirement stands
41	RFP No.	12	3	All solutions to be in HA mode in DC & standalone mode in DR/NDR.	Request for Clarification : Please confirm whether bidder need to deploy NAC Solution in both PDCC High availability in DC and standalone in DR locations? Whether it will be, will the deployment requirement 1) HA in DC 2)Standalone in DR	Understanding is correct
42	RFP No.	12		Network Access Control (NAC) (Existing user count is approximately 2500 and components count is 2300)	Request for Clarification : In the RFP, 2300 component are mentioned. Are we included guest count details? If it is not please mentioned the guest device or user details?	Guest devices are prohibited in PDCC environment.
43	2.1	13	Point 9	9. Log has to be retained for a period of Six (6) months Online and additional Six (6) months offline. SIEM should collect log from all solutions as per above mentioned table "Assets to be integrated for CSOC" and provide a comprehensive picture. If bank procures any additional devices/solutions/Services during the tenure of contract the same should be integrated in SIEM without any additional cost to the Bank.	1) We offer 3 months online and 9 months offline storage as per industry standards. Hope this is fine. 2) Integrating/On-boarding additional devices required manual efforts depending on the number of log sources & will attract additional cost. Pls confirm if this is fine.	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
44	2.1	13	Point 13	The Bidder is expected to size the Hardware/appliance/storage as per the requirements mentioned in this RFP which will be seamlessly work for 5 years.	Kindly provide the estimated year on Year growth % for next 5 Year in term of Branches, User, Data(In TB),	10% Y-o-Y growth.
45	2. Detailed Scope of Work	13	34	16. Integrate the C-SOC solutions with proposed application platforms, server and storage environment, enterprise network, EMS/ NMS solutions, security solutions, ticketing tools etc.	Request for clarification: Will the bidder have to integrate its ITSM with Banks ticketing solution for CSOC tickets monitoring?	Not required.
46	2. Detailed Scope of Work	13	28	28. Provide forensics support as per the requirement of Bank in case of any incident.	Request for clarification: forensic support is a needs basis service also termed as Digital forensics and incident response services (DFIR) So request the Bank to clarify how many hrs. per year of forensics support are to be factored. *Justification: Asking for the Bill of Material for forensics support this service will help the bank to compare the overall quotes received from various bidders and the evaluation will be transparent.* *for example: the Bank may ask for 40 hrs. of DFIR services per year.*	Kindly refer Annexure 11: Bill of Material for detail clarification

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
47	2. Detailed Scope of Work	13	34	34. The Bidder would be responsible for updates, patches, bug fixes, version upgrades for the entire infrastructure without any additional cost to the Bank during the contract period.	Request for clarification: Please confirm if our understanding is correct that responsibilities for updates, patches, bug fixes, version upgrades for the entire infrastructure is only for the new proposed CSOC solution part of this RFP and not for any other Banks existing security tools or solution ?	Understanding is correct
48	2.1	13	12	The proposed backup target should be disk based hardware solution	The Clause only mentions about the backup target, please confirm if Bank will provide the required Backup software for taking the backup	Bidder to propose cost effective solution.
49	2.1	13	12	The proposed backup target should be disk based hardware solution	Please confirm the backup policy and the retention period for the backup solution	It will be discussed with Final selected bidder.
50	2.1	13	11	The bidder should provide 42U rack to mount the proposed solutions at Bank's DC & DR (colocation charges will be Borne by Bank). However, the procurement of the rack will be finalized with the selected bidder	Hope bank to take care of the rack in the NDR location, as it is not asked in the RFP	Understanding is correct
51	2.1	14	Point 27	The VAPT solution integrates seamlessly with SIEM to provide real time alters and comprehensive analysis and ensure the tool can perform security assessments on mobile applications across different platforms like Android and iOS. Frequency for VAPT audit will be Half yearly once, as and when required.	1)Is the expectation to integrate VAPT report/findings with SIEM Tool? 2)is the VAPT exercise expected to be conducted continuously (Since real-time alert is required) or VAPT has to be performed Once every Half year 3) Pls specify the total number of mobile applications to be consider for VAPT 4) Pls specify the total number of Web applications to be consider for VAPT	It will be discussed with selected bidder.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
52	2.1	14	Point 19	19 The bidder should provide Ticketing tool from their CSOC	Do you need any additional integration with your ITSM Tool	Not required to be integrated.
53	2.1	14	Point 18	Integrate the C-SOC solutions with proposed application platforms, server and storage environment, enterprise network, EMS/ NMS solutions, security solutions, ticketing tools etc	Pls specify that EMS/NMS Solution need to be provided by bidder or not	No EMS/NMS to be provided by bidder. Bidder to provide ticket tool access for CSOC operations.
54	2.1	14	Point 21	Development of operating procedures in adherence PDCC's policies.	Kindly share PDCC Policies, to be consider in Scope	It will be shared with Final selected bidder.
55	2.1	14	Point 28	The bidder should do the hardening of the proposed hardware and applications after successful implementation	Kindly confirm which specific Hardening Guideline are to be followed	Hardening of the proposed hardware and applications after successful implementation should be as per RBI/NABARD guidelines
56	2.1	14	Point 31	Ensure adherences to Bank's Information Security Policy, Cyber Security Policy and Cyber Crises Management Plan etc.	Kindly share the Bank Polices to be adhered	It will be shared with Final selected bidder.
57	2.1	15	Point 36	Ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the provided locations by Bank), enhancements, updates, upgrades, bug fixes, backups, audits, on-site as well as off-site support for the proposed hardware/software required for delivering the proposed Security services.	Can you confirmed this Scope only limited only to device managed by the Service provider. Not Consider the End Point , Firewall Management etc.	Please be guided by RFP.
58	2.1	15	Point 45	Virus alerts through SMS/e-Mail for the viruses, worm's activity observed at the security solutions and devices under the Bidder scope. Subsequent activities of remediation & closure are the responsibility of Antivirus service provider. Bidder will track the status of	Is it expected from Service Provider to coordinate with the OEM for remediation	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				the Trouble Ticket opened in this context.		
59		15	40	The system should be in high-availability mode at Log collection and Logger level and with BC (Business Continuity) set-up at Bank's DR (Disaster Recovery) & NDR site.	Request for Clarification: In the RFP, it is clearly mentioned bidder to provide Managed SOC Services for SIEM, Anti-Phishing , Dark Web and SOAR. This DC-DR replication functionality is relevant for On Prem DC - DR Deployment of SIEM, Anti-Phishing , Dark Web and SOAR. Justification: Still, if the Bank needs DC-DR replication functionality, then they've to go with DC-DR On Prem setup. Please suggest what could be the expected offerings from the bidder?	The system should be in high-availability mode at Log collection and Logger level and with BC (Business Continuity) set-up at Bank's DR (Disaster Recovery) for On premises services.
60		15	36	Ensure that all aspects of Installation, De-Installation, integration, Configuration, Re-configuration, relocation (within the provided locations by Bank), enhancements, updates, upgrades, bug fixes, backups, audits, on-site as well as off-site support for the proposed hardware/software required for delivering the proposed Security services.	Request for Clarification: With reference to RFP Document page no. 9, under The solutions that are already available at Bank states, Commvault Backup tool in PDCC. Justification : Using the existing backup tool will help Bank to save cost and have optimize solution in place for the new proposed solution's backup as Bank is already having similar solution deployed. We can recommend the additional upgrade require in existing backup tool.	Bidder to propose cost effective solution.
61	2.1	16	Point 51	Solution should cover Phishing simulation and training module to educate bank users and test their response to phishing attacks.	What will the Schedule for is the Phishing Simulation & for How many user, /Monthly Quarterly/ Yearly	It will be discussed with selected bidder.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
62	2.1	16	Point 55	The solution for Patch, Software and Hardware asset inventory management broadly covers Windows, Unix, Linux, Ubuntu etc.	Do you have any existing Patch Management Tool	Kindly Refer Point No 2. Detail Scope of Work
63	2.1	16	Point 51	Solution should cover Phishing simulation and training module to educate bank users and test their response to phishing attacks.	Kindly confirm the number of User for Phishing simulation & what is frequency.	It will be discussed with Final selected bidder.
64	2.1	16	47	For DC-DR replication, the solution should also have the capabilities to replicate it during non-business hours. Bidder to confirm the capacity of DC-DR replication link required for CSOC operations and bank will enhance DC-DR replication link accordingly.	What kind of replication is expected, is it on the application level or storage level?	Bidder to propose the solution based on the RFP.
65		16	47	For DC-DR replication, the solution should also have the capabilities to replicate it during non-business hours. Bidder to confirm the capacity of DC-DR replication link required for CSOC operations and bank will enhance DC-DR replication link accordingly.	Request for Clarification: In the RFP, it is clearly mentioned bidder to provide Managed SOC Services for SIEM, Anti-Phishing , Dark Web and SOAR. This DC-DR replication functionality is relevant for On Prem DC - DR Deployment of SIEM, Anti-Phishing , Dark Web and SOAR. Justification: Still, if the Bank needs DC-DR replication functionality, then they've to go with DC-DR On Prem setup. Please suggest what could be the expected offerings from the bidder?	The system should be in high-availability mode at Log collection and Logger level and with BC (Business Continuity) set-up at Bank's DR (Disaster Recovery) for On premises services.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
66	RFP	16	51	Solution should cover Phishing simulation and training module to educate bank users and test their response to phishing attacks.	Request for Clarification: Please suggest total no. of users to be factored for this phishing simulation tool. Please update the Annexure 11 Commercial Bill of Material for costing and services required duration(monthly/quarterly/annually)	All users to be factored atleast once in 6 months. Phishing Simulation and training should be the part of proposed solution.
67	2.2	17	Point 8. Onsite CSOC Management	1 resource in bank working hours	Pls specify the bank working hours	Bank working hours are 9am to 7pm
68	RFP	17	2	Onsite FMS team proactively looks for signs of malicious activity in a Banks network with the help of tools and techniques to identify threats that automated systems might miss. Also, should collaborate with other cyber security teams and share findings and methodologies.	Request for Clarification: To Achieve this requirement, bidder needs to suggest dedicated threat hunter skilled resource at banks premises or remotely. Please confirm the feasible option Please update the Annexure 11 Commercial Bill of Material for costing and services required duration.	RFP requirement stands
69	RFP	17	4	It is bidders' responsibility to manage the overall FMS services by deploying additional resources without any additional cost to the bank in the absence/leave of L1/L2 in their leave and holidays, otherwise the number of leaves amount will be deducted from FMS billing.	Request for Modification: To cover the full scope of services and tools mgmt. for the proposed solutions in PDCC premises at minimum the bidder is required to provide "FM Services" with the below quantities. Facility Management Resources HO L2 : 2 Nos. Facility Management Resources HO L1 : 6 Nos.	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
70	3.1	19	Eligibility Criteria	A. GENERAL	Please add in RFP: The bidders (including MSE) or Bidder’s Parent Company (in case bidder is a 100% wholly owned subsidiary of parent company) should be a registered company in India as per Companies Act 1956 / 2013 and must have been in running SOC operations Business for a period of at least 7 years (as on RFP date)	RFP Requirement Stands
71	3.1	19	Eligibility Criteria	A. GENERAL (point2) The bidder should have ISO 9001:2015, minimum CMMi Level 3 certified, ISO 27001:2013/ ISO27001:2022	Change to: CMMi Level 5	RFP Requirement Stands
72	3.1	19	Eligibility Criteria	A. GENERAL (point4) The Bidder should have its own managed Cyber SOC along with its DR site in India.	The Bidder should have its own managed Cyber SOC along with its DR site in India. Add : Remote Security Operations Center should be SOC1, SOC2, SOC3 compliant. Certificates should be provided	RFP Requirement Stands
73	3.1	19	Eligibility Criteria	B. FINANCIAL (Point 1) The bidder should have a minimum annual average turnover of INR 100 Crore for each of the 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24) exclusively from their Indian operations.	Change to: The bidder should have a minimum annual average turnover of INR 500 Crore for each of the 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24)	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
74	C	20	C. EXPERIENCE & SERVICE CAPABILITY	Service Model: The bidder should provide the CSOC services from MeitY empaneled Government community cloud infrastructure i.e., SIEM/SOAR/ DLP/PIM etc., Solution should be hosted with MeitY empaneled government community cloud.	a. We have full-fledged NG-SOC deployed on our private cloud in Mumbai which we leverage to provide Platform based SOC services to our large clientele in BFSI. The platform has all relevant certifications and is also MEITY empaneled. As per your eligibility criteria, we are not qualifying on your prerequisite that the service provider's SOC has to be on GCC platform. Please confirm if we can submit our bid based on delivery from our SOC which is MEITY empaneled but not on GCC cloud. b. If above point is not acceptable, please confirm if we can provide all the services in RFP on on-site model i.e. completely from PDCCB's premise.	Revised Clause: Service Model: The bidder should provide the CSOC services from MeitY empaneled cloud infrastructure i.e., SIEM/SOAR/ DLP/PIM etc., Solution should be hosted with MeitY empaneled cloud.
75	3.1	20	Eligibility Criteria	B. FINANCIAL (Point 2) The bidder should be a Profit-making company for any 3 out of 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24) from the India operations. Profit After Taxes (PAT) will be considered	Change to: The bidder should be a Profit-making company for all 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24) from the India operations. Profit After Taxes (PAT) will be considered	RFP Requirement Stands
76	3.1	20	Eligibility Criteria	B. FINANCIAL (Point 3) The bidder should have positive net worth in any 3 out of 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24).	Change to: The bidder should have positive net worth in all 4 financial years (2020-21, 2021-22, 2022-23 & 2023-24).	RFP Requirement Stands
77	3.1	20	Eligibility Criteria	The bidder should have prior experience of the Implementation & management of CSOC for at least One (1) bank in India in the last 3 years.	The bidder should have prior experience of the Implementation & management of CSOC for at least One (1) bank in India in the last 5 years for minimum 50000 EPS.	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
78	3.1	20	Eligibility Criteria	Bidder should have registered office in India and should have implemented own Security Operation Center or should be managing CSOC setup within India.	Bidder should have registered office in India and should be providing Managed Security Services from MSSP location in India for minimum 10 BFSI Customers	RFP Requirement Stands
79	3.1	20	Eligibility Criteria	C. EXPERIENCE & SERVICE CAPABILITY (Point 3) Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR.	Change to: Bidder should have at least 50 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR.	RFP Requirement Stands
80	3.1	20	C. EXPERIENCE & SERVICE CAPABILITY	Service Model: The bidder should provide the CSOC services from MeitY empaneled Government community cloud infrastructure i.e., SIEM/SOAR/ DLP/PIM etc., Solution should be hosted with MeitY empaneled government community cloud.	Understanding is the DLP solution is already existing with PDCC Bank. However as per this clause, kindly confirm bidder has to provide DLP solution or not	Kindly refer RFP Clause: 2. Detailed Scope of Work
81	Detailed Technical Evaluation Parameters:	24	Sr. No. 2 Bidder' s capability and experience	➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Seven (7) or more mandatorily including SIEM and SOAR from the below-proposed solutions in one bank for each item in India in the last 5 years. b. 7 Marks: If the bidder provides credentials for at least Four (4) mandatorily including SIEM and SOAR from the below- proposed solutions in	We request you to amend the clause as; ➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a bank /BFSI/Govt organization in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Seven (7) or more mandatorily including SIEM and SOAR from the below-proposed solutions in one bank /BFSI /Govt organization for each item in India in the last 5 years. b.7 Marks: If the bidder provides	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				one bank for each item in India in the last 5 years. The proposed solutions are: 1. Network Access Control (NAC), 2. Endpoint Detection Response (EDR), 3. Endpoint Forensic and Behavior Analysis (EFBA), 4. Database activity monitoring (DAM), 5. Security information and event management (SIEM) 6. Privileged identity and Access management (PIM/PAM) 7. Network Behavior Anomaly Detection (NBAD) 8. Threat Intelligence (as service) 9. SOAR 10. VAPT tool as per NABARD guidelines 11. Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge and Dark web monitoring Note: If the bidder does not have a single credential mentioning above all components in a bank, the bidder is free to provide credentials from atleast one bank for each of the identified components separately which includes SIEM and SOAR.	credentials for at least Four (4) mandatorily including SIEM and SOAR from the below- proposed solutions in one bank/BFSI/Govt organization for each item in India in the last 5 years. The proposed solutions are: 1. Network Access Control (NAC), 2. Endpoint Detection Response (EDR), 3. Endpoint Forensic and Behavior Analysis (EFBA), 4. Database activity monitoring (DAM), 5. Security information and event management (SIEM) 6. Privileged identity and Access management (PIM/PAM) 7. Network Behavior Anomaly Detection (NBAD) 8. Threat Intelligence (as service) 9. SOAR 10. VAPT tool as per NABARD guidelines 11. Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge and Dark web monitoring Note: If the bidder does not have a single credential mentioning above all components in a bank/BFSI/Govt organization, the bidder is free to provide credentials from atleast one bank for each of the identified components separately which includes SIEM and SOAR.	

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
82	4.5	24	Technical Evaluation: Bidder’s capability and experience	The bidder should have prior experience of the Implementation & management of CSOC for at least One (1) bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for three (03) or more banks in India out of which one should be State Cooperative or DCCB/ Schedule Commercial Bank/ PSU in the last 5 years.	The bidder should have prior experience of the Implementation & management of CSOC for at least One (1) bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for three (03) or more banks / PSU / BFSI in India out of which one should be State Cooperative or DCCB/ Schedule Commercial Bank/ PSU / BFSI in the last 5 years.	RFP Requirement Stands
83	4.5	24	Technical Evaluation: Bidder’s capability and experience	The bidder should have prior experience in the Implementation of the mentioned solutions in a bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Seven (7) or more mandatorily including SIEM and SOAR from the below- proposed solutions in one bank for each item in India in the last 5 years.	The bidder should have prior experience in the Implementation of the mentioned solutions in a bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Six (6) or more mandatorily including SIEM from the below-proposed solutions in one bank for each item in India in the last 5 years.	RFP Requirement Stands
84	4.5	24	Technical Evaluation: Bidder’s capability and experience	Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR. a. 10 Marks: If the bidder provides declaration for more than 10 certified CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR resources under the company's payroll along with the CV and certificates.	Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR. a. 10 Marks: If the bidder provides declaration for more than 50 certified CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM/SOAR resources under the company's payroll along with the CV and certificates.	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
85	4.5	24	Technical Evaluation: Bidder’s capability and experience	Bidder should have currently in the business of providing CSOC/ SOC managed security services including log monitoring and correlation for minimum 500 assets and 3000 EPS in atleast one Bank in India. a. 10 Marks: If the bidder provides credentials for three (03) or more banks in India.	Bidder should have currently in the business of providing CSOC/ SOC managed security services including log monitoring and correlation for minimum 10000 EPS in atleast one Bank / PSU / BFSI in India. a. 10 Marks: If the bidder provides credentials for three (03) or more banks/PSU/BFSI in India.	RFP Requirement Stands
86	4.5	24	Technical Evaluation: Bidder’s capability and experience	Dark web monitoring	How may Domain & sub domain and Brands to be consider for Dark web Monitoring	Approximately 3 Domains and 10 Sub domains.
87	4.5	24	Technical Evaluation: Bidder’s capability and experience	Endpoint Detection Response (EDR),	1) Does EDR required for both Endpoint & Server 2) If Required for Both, pls share the count of endpoint & server to be consider 3) Kindly specify all the endpoint OS in Scope 4) Kindly specify all the Server OS on Scope	1) Yes, EDR required for both 2) Existing user count is approximately 2500 3) All Non-End of Support Windows versions 4) All Non-End of Support Windows & Redhat Linux versions
88	Bidder’s capability and experience	24	2	➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Seven (7) or more mandatorily including SIEM and SOAR from the below- proposed solutions in one bank for each item in India in the last 5 years. b. 7 Marks: If the bidder provides credentials for at least Four (4) mandatorily including SIEM and SOAR from the below- proposed	We request PDCC to modify the clause as below:- ➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for at least Seven (7) or more ~~mandatorily including SIEM and SOAR~~ from the below~~- proposed~~ solutions in one bank for each item in India in the last 5 years. b. 7 Marks: If the bidder provides credentials for at least Four (4) ~~mandatorily including SIEM and~~	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				solutions in one bank for each item in India in the last 5 years. The proposed solutions are: 1. Network Access Control (NAC), 2. Endpoint Detection Response (EDR), 3. Endpoint Forensic and Behavior Analysis (EFBA), 4. Database activity monitoring (DAM), 5. Security information and event management (SIEM) 6. Privileged identity and Access management (PIM/PAM) 7. Network Behavior Anomaly Detection (NBAD) 8. Threat Intelligence (as service) 9. SOAR 10. VAPT tool as per NABARD guidelines 11. Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge and Dark web monitoring Note: If the bidder does not have a single credential mentioning above all components in a bank, the bidder is free to provide credentials from atleast one bank for each of the identified components separately which includes SIEM and SOAR.	~~SOAR~~ from the below~~- proposed~~ solutions in one bank for each item in India in the last 5 years. The ~~proposed~~ solutions are: 1. Network Access Control (NAC), 2. Endpoint Detection Response (EDR), 3. Endpoint Forensic and Behavior Analysis (EFBA), 4. Database activity monitoring (DAM), 5. Security information and event management (SIEM) 6. Privileged identity and Access management (PIM/PAM) 7. Network Behavior Anomaly Detection (NBAD) 8. Threat Intelligence (as service) 9. SOAR 10. VAPT tool as per NABARD guidelines 11. Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge and Dark web monitoring Note: If the bidder does not have a single credential mentioning above all components in a bank, the bidder is free to provide credentials from atleast one bank for each of the identified components separately which includes SIEM and SOAR.	

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
89	Detailed Technical Evaluation Parameters:	25	Sr. No. 2 Bidder' s capability and experience	➢ Bidder should have currently in the business of providing CSOC/ SOC managed security services including log monitoring and correlation for minimum 700 assets and 5000 EPS in atleast one Bank in India. a. 10 Marks: If the bidder provides credentials for three (03) or more banks in India. b. 7 Marks: If the bidder provides credentials for less than three (03) banks in India.	We request you to kindly amend the clause as: ➢ Bidder should have currently in the business of providing CSOC / SOC managed security services including log monitoring and correlation for minimum 100 assets and 3000 EPS in any BFSI/PSU across India. a. 10 Marks: If the bidder provides credentials for atleast three (03) or more BFSI/PSU in India. b. 7 Marks: If the bidder provides credentials for less than three (03) BFSI/PSU in India.	RFP Requirement Stands
90	RFP	28	4	For the purpose of availability, the service window will be 24*7*365. Parameters : availability of CSOC Solution	Request for Clarification: To comply with the SLA expectations as per PDCC requirement minimum the bidder is required to provide "FM Services" with the below quantities. Facility Management Resources HO L2 : 2 Nos. (General Shift) Facility Management Resources HO L1 : 6 Nos. (24/7)	RFP requirement stands
91	RFP	29	5.3	Helpdesk Response	Request for Clarification: What is helpdesk tool bank is currently using? Will bank extend the existing helpdesk/ITSM for the bidder proposed FMS resources? If not, then please suggest whether bidder needs to setup helpdesk in banks premises. Please update the Annexure 11	Kindly refer RFP Clause: 5.3 Helpdesk Response

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					Commercial Bill of Material for costing and services required duration.	
92	6.10 Bid Security – Earnest Money Deposit	35	1	The bidder shall furnish as part of its bid, bid security of INR 10,00,000/- (Rupees Ten Lakhs Only).	Request PDCC to please confirm whether we need to submit a new EMD in the form of a Bank Guarantee, or if the previously submitted Bank Guarantee will be considered?	It has been communicated separately over email/call.
93	6.11 Performance Bank Guarantee	36	1	Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) amounting to 7% of the total project cost for 5 years 6 months (including 6 months transition phase) and valid for 66 months including claim period of 6 (six) months, validity starting from its date of issuance. the PBG shall be submitted within 15 days from the acceptance of the Purchase Order.	Bidder will furnish an unconditional and irrevocable Performance Bank Guarantee (PBG) amounting to 5% of the total project cost for 5 years 6 months (including 6 months transition phase) and valid for 66 months including claim period of 6 (six) months, validity starting from its date of issuance. the PBG shall be submitted within 15 days from the acceptance of the Purchase Order.	RFP requirement stands
94	6.20 Limitation of Liability	39	6.2	The aggregate liability of the bidder in connection with this Agreement, the services provided by the bidder for the specific RFP document, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise) and including any and all liability shall be the actual limited to the extent of the total contract value.	We propose to add below mentioned language to the existing clause: NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, OR LOSS OF DATA, OR INTERFERENCE WITH BUSINESS, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.	
95	6.32	43	Exit Management	Bidder has to provide support during migration activities to the new Bidder of PDCC Bank.	Kindly confirm the Total Scope of Migration Activity	It will be shared with Final selected bidder.
96	6.34 Transfer of Documents	44	6.34.1 Transfer of Agreements	On request by PDCC Bank or its selected service provider or any other agency, Bidder shall affect such assignments, transfers, innovations, licenses and sub-licenses in favor of PDCC Bank or its nominated service provider or any other agency, in relation to any equipment lease, maintenance or service provision agreement between Bidder and selected service provider or any other agency, and which are related to the services and reasonably necessary for the carrying out replacement services.	We Request you to kindly amend the clause as: On request by PDCC Bank or its selected service provider, bidder shall affect such assignments and transfers in favor of PDCC Bank or its nominated service provider, in relation to any equipment lease, maintenance or service provision agreement between Bidder and selected service provider or any other agency, and which are related to the services and reasonably necessary for the carrying out replacement services.	RFP Requirement Stands
97	6.39 Penalty	46	6.39	The proposed rate of penalty is as mentioned in Service levels with an overall aggregate cap of penalty to be limited to 10% of contract value.	The proposed rate of penalty is as mentioned in Service levels with an overall aggregate cap of penalty to be limited to 5% of contract value.	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
98	7 Payment Terms	47	7	1. Hardware Cost a. 50% of the delivered hardware cost would be payable on delivery. b. 20% of the hardware cost would be payable on post installation. c. 20% of the hardware cost would be payable after Go-live on production environment. d. 10% of the cost would be payable on completion of 3 months from the date of successful setting up of the tools and sign off by the bank. 2. Hardware & software implementation/ installation cost a. Implementation/installation cost will be paid after 30 days of successful implementation, sign off and acceptance by the bank. 3. Software License cost a. 70% of the license cost will be paid on delivery of licenses of applications, installation and after sign -off from the bank b. 30% of the license cost will be paid after successfully go live and setting up of the application and sign off by the bank. 4. One Time Charges – One-time charges (if any) for installation and configuration for all CSOC components will be paid after successful installation, configuration, signoff and acceptance by the Bank. 5. AMC & ATS Cost of Hardware/ Software a. ATS & AMC cost for Hardware will be	Hardware Cost a. 80% of the delivered hardware cost would be payable on delivery. b. 10% of the hardware cost would be payable on post installation. c. 5% of the hardware cost would be payable after Go-live on production environment. d. 5% of the cost would be payable on completion of 3 months from the date of successful setting up of the tools and sign off by the bank. 2. Hardware & software implementation/ installation cost a. Implementation/installation cost will be paid after 30 days of successful implementation, sign off and acceptance by the bank. a. Phase wise payment Phase- I 30% Basic installation of H/w & S/w b. Phase -II 40% Integration of solutions c. Phase -III 20% UAT Sign Off d. Phase IV 10% Go Live 3. Software License cost a. 90% of the license cost will be paid on delivery of licenses. b. 10% of the license cost will be paid after successfully go live and setting up of the application and sign off by the bank. 4. One Time Charges – One-time charges (if any) for installation and configuration for all	RFP requirement stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				paid half yearly in arrears. b. ATS/AMC documents for in-scope software and hardware from the OEM for service and support have to be provided to the bank. Payment will be made on submission of these document. 6. FM Resource Cost a. The annual amount to be paid towards FM services cost would be divided into 4 equal instalments, to be paid quarterly at the end of each quarter. The first quarter would begin after successful completion of the transition.	CSOC components will be paid after successful installation, configuration, signoff and acceptance by the Bank. a. Phase- I 40% Basic installation of H/w & S/w b. Phase -II 30% Integration of solutions c. Phase -III 20% UAT Sign Off d. Phase IV 10% Go Live 5. AMC & ATS Cost of Hardware/ Software a. ATS & AMC cost for Hardware will be paid yearly in Advance. b. ATS/AMC documents for in-scope software and hardware from the OEM for service and support have to be provided to the bank. Payment will be made on submission of these document. 6. FM Resource Cost a. The annual amount to be paid towards FM services cost would be divided into 4 equal instalments, to be paid quarterly at the end of each quarter. The first quarter would begin after successful completion of the transition.	
99	7	48	Payment Terms	7.5 AMC & ATS Cost of Hardware/ Software	Please change the payment terms to Yearly advance	RFP Requirement Stands
100	7	48	Payment Terms	7.6 FM Resource Cost	Please change to The annual amount to be paid towards FM services cost would be divided into 4 equal instalments, to be paid quarterly in advance.	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
101	7	48	Payment Terms		SIEM, Dark Web Monitoring, SOAR will be delivered as part of services. Please have separate payment terms for them as "amount to be paid Quarterly in Advance"	RFP Requirement Stands
102	8.10 Annexure 10: Functional and Technical Specification "Annexure 10 Functional and Technical Requriement. xls"	64	Excel Spreadsheet for SOAR - Sl. No. 2	SOAR must be integrated platform with SIEM on same user interface	We Request you to kindly amend the clause as: SOAR must be integrated platform and change same user interface to easily navigate to SOAR Interface	Revised Clause: SOAR must be integrated platform with SIEM to comply with minimum requirement mentioned in RFP.
103	8.10 Annexure 10: Functional and Technical Specification "Annexure 10 Functional and Technical Requriement. xls"	64	Excel Spreadsheet for NBAD	All Technical Requirement Points	NBAD is an OEM specific hardware/appliance based solution. Hence requesting to remove NBAD and introduce generic functionalities of NDR solution that can be integrated with bidder CSOC SIEM solution/console.	RFP Requirement Stands
104	SOAR Compliance(Annexure 10 funcation and technical requirements)	Annexure 10	2	SOAR must be integrated platform with SIEM on same user interface	Change Request: This functionality "SOAR must be integrated platform with SIEM on same user interface" is only possible if the proposed SIEM and SOAR solutions are from the same OEM. We suggest the SOAR and SIEM should integrate to made the functional requirements instead of having same	Revised Clause: SOAR must be integrated platform with SIEM to comply with minimum requirement mentioned in RFP.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					dashboard. Justification: This will be a restrictive clause for us to comply with our MSOC services as we are proposing our MSOC model as per RFP requirements, our proposed SIEM and SOAR solutions are IBM Qradar and PaloAlto Cortex XSOAR and these are different OEMs, thus providing the industry's best-of-breed solutions.	
105	Annexure 10 EDR Compliance(Annexure 10 functional and technical requirements)	EDR	23	The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on both monitored and non-monitored systems.	Request for Modification : This is not a EDR Specific feature. Kindly remove this for wider participation.	Revised Clause: The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on monitored systems.
106	EDR Compliance(Annexure 10 functional and technical requirements)	EDR	40	The solution should show the IP addresses and host names from hosts file on Windows, Linux, and macOS devices.	Request for Modification: Requesting tendering committee to remove the Linux and MAC OS Support for the proposed EDR solution. Justification : In most of the EDR/Endpoint security solutions Linux and MAC OS platforms are not supported also the features and functionality for anti-malware is not available with most of the well known OEMs in this category. Hence we again request to remove support for Linux and Mac OS platforms for wider participations.	Revised Clause: The solution should show the IP addresses and host names from hosts file on Windows & RedHat Linux.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
107	EDR Compliance(Annexure 10 functional and technical requirements)	EDR	44	The solution should support Windows, Linux and MacOS	Request for Modification: Requesting tendering committee to remove the Linux and MAC OS Support for the proposed EDR solution. Justification : In most of the EDR/Endpoint security solutions Linux and MAC OS platforms are not supported also the features and functionality for anti-malware is not available with most of the well known OEMs in this category. Hence we again request to remove support for Linux and Mac OS platforms for wider participations.	Revised Clause: The solution should support Windows & RedHat Linux.
108	EDR Compliance(Annexure 10 functional and technical requirements)	EDR	50	The solution should be able to run a vulnerability scan on a particular endpoint if under investigation.	Request for Modification : This is not a EDR Specific feature. Kindly remove this for wider participation.	Please consider the clause as deleted
109	Annexure 10 Functional and Technical Requirements	NAC		The solution should not allow infection of already quarantined elements by other quarantined elements.	Request for clarification: Please elaborate for our understanding	Quarantined elements to be logically separated from each other to avoid infection.
110	Annexure 10 Functional and Technical Requirements	NAC		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 etc.	Request for clarification: Please share the list of all the third party devices with device type, make, model number.	Please refer RFP Section 2: Detailed Scope of Work. Model nos will be shared with selected bidder.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
111	Annexure 10 Functional and Technical Requirements	NAC		VLAN Steering, DHCP, Anti ARP spoofing, Span Ports, Agent based enforcement, HTTP User Agent, Mac Authentication, MAC OUI and TCP SYN-ACK handshakes etc.	Request for clarification: We understand that policy validation is nothing but the device profiling mechanisms. Forti NAC will comply by using profiling for policy validation. Please confirm that the bank is okay with this setup.	Bidder to comply RFP requirement
112	Annexure 10 Functional and Technical Requirements	NAC		The solution should be able to provide visibility to VPN users as well	Request for clarification: We understand that perimeter firewall has capability to integrate with FortiNAC over Radius. FortiNAC will comply by integrating with firewall. Please confirm that the bank is okay with this setup.	Understanding is correct
113	Annexure 10 Functional and Technical Requirements	NAC		The solution should support Microsoft NAP and Trusted Computing Group.	Request for clarification: Since the RFP is for a dedicated NAC solution which already profiles and does compliance checks of all the devices connecting to the network, what use case are we trying to achieve with Microsoft NAP.	Please consider the clause as deleted
114	Annexure 10 Functional and Technical Requirements	NAC		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 for clarification: How many IOC sources are available with the bank. Just to understand the setup.	It will be discussed with Final selected bidder.
115	Annexure 10 Functional and Technical Requirements	NAC		The solution should be able detect and manage hand held devices used for financial inclusion process.	Request for clarification: Please elaborate these lines for our understanding	Micro ATM devices

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
116	Annexure 10 Functional and Technical Requirements	NBAD	1.1	Proposed NBAD Systems should be hardware-based appliances.	Request for clarification: Please confirm if Bank is looking for NBAD solution which is Appliance based only or we can also provide Server based NBAD solution (Software deploy on the Server Hardware) ?	NBAD can be hardware or software based
117	Annexure 10 Functional and Technical Requirement	NBAD	1.1	Proposed NBAD Systems should be hardware-based appliances.	Request for clarification: Kindly share the below volumetrics for proposing the sizable NBAD solution required by bank: - FPS (Flows Per Second) or - Throughput in Gbps	Current Network throughput is around 750 Mbps.
118	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	1.1	Proposed NBAD Systems should be hardware-based appliances.	Request for Clarification : Please confirm whether bidder need to deploy NBAD Solution in both PDCC DC and DR locations? Whether it will be, will the deployment requirement 1) Active - Passive , HA in both in DC and DR? Or 2) HA in both DC and DR Standalone? Or 3) Active in DC Standalone and Passive in DR Standalone?	The Bidder shall consider implementation of bank-end CSOC components at Bank’s DC (in HA mode) & DR (In Standalone mode) only. CSOC should monitor entire Bank’s infrastructure including the NDR.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
119	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	2.3	The Solution should be able to detect Malwares on both encrypted and nonencrypted payloads.	Request for Clarification: With reference to RFP Document page no. 9, Point 11. states, there is SSL Interceptor (Array) in PDCC. Now, for the complete functionality of proposed NBAD solution there would be required for SSL decrypter solution to scan the encrypted traffic. In that case, as Bank is already having similar solution deployed in their environment will Bank extend the functionality with the proposed NBAD Solution? Justification : with the clarity, whether bidder need to propose the SSL appliances required for NBAD or not. This will help Bank to save cost and have optimize solution in place for the new proposed NBAD solution as Bank is already having similar solution deployed.	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
120	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	4.14	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility	Request for Clarification: With reference to RFP Document page no. 9, Point 11. states, there is SSL Interceptor (Array) in PDCC. Now, for the complete functionality of proposed NBAD solution there would be requirement for SSL decrypter solution to scan the encrypted traffic. In that case, as Bank is already having similar solution deployed in their environment will Bank extend the functionality with the proposed NBAD Solution? Justification : with the clarity, whether bidder need to propose the SSL appliances required for NBAD or not. This will help Bank to save cost and have optimize solution in place for the new proposed NBAD solution as Bank is already having similar solution deployed.	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
121	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	4.41	The solution should support detection of malware in Encrypted traffic through analytics.	Request for Clarification: With reference to RFP Document page no. 9, Point 11. states, there is SSL Interceptor (Array) in PDCC. Now, for the complete functionality of proposed NBAD solution there would be requirement for SSL decrypter solution to scan the encrypted traffic. In that case, as Bank is already having similar solution deployed in their environment will Bank extend the functionality with the proposed NBAD Solution? Justification : with the clarity, whether bidder need to propose the SSL appliances required for NBAD or not. This will help Bank to save cost and have optimize solution in place for the new proposed NBAD solution as Bank is already having similar solution deployed.	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
122	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	4.42	The solution is capable of performing Encrypted Traffic Analytics to predict with a high level of accuracy whether or not an encrypted flow session is likely to be hiding threat vectors.	Request for Clarification: With reference to RFP Document page no. 9, Point 11. states, there is SSL Interceptor (Array) in PDCC. Now, for the complete functionality of proposed NBAD solution there would be requirement for SSL decrypter solution to scan the encrypted traffic. In that case, as Bank is already having similar solution deployed in their environment will Bank extend the functionality with the proposed NBAD Solution? Justification : with the clarity, whether bidder need to propose the SSL appliances required for NBAD or not. This will help Bank to save cost and have optimize solution in place for the new proposed NBAD solution as Bank is already having similar solution deployed.	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
123	NBAD Compliance(Annexure 10 functional and technical requirements)	NBAD	4.43	The solution should be able to detect Unknown or encrypted malware, insider threats, policy violations.	Request for Clarification: With reference to RFP Document page no. 9, Point 11. states, there is SSL Interceptor (Array) in PDCC. Now, for the complete functionality of proposed NBAD solution there would be requirement for SSL decrypter solution to scan the encrypted traffic. In that case, as Bank is already having similar solution deployed in their environment will Bank extend the functionality with the proposed NBAD Solution? Justification : with the clarity, whether bidder need to propose the SSL appliances required for NBAD or not. This will help Bank to save cost and have optimize solution in place for the new proposed NBAD solution as Bank is already having similar solution deployed.	Yes. Understanding is correct
124	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should discover all databases in Bank environment at time of implementation and further any rogue/new database and dB objects created within the monitored network/system and should send the real time alert to respective security staffs.	Additional clause not accepted.
125	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should able to auto classify the database/database-objects based on sensitivity and confidentiality of data based on PII, SPDI, PCI DSS guidelines or customized parameters.	Additional clause not accepted.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
126	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should be capable of auto discovering sensitive/confidential data, like credit card Numbers, Email address Aadhaar or any PII in the database and offers the ability for customization.	Additional clause not accepted.
127	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc.	The solution should monitor DDL, DML, DCL, TCL, and DQL commands in real-time and It should also monitor user management, privilege management etc. and monitor for any policy violations.	Additional clause not accepted.
128	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc.	The solution should work in monitor-only and blocking mode to protect the application from any immediate threat as per the Bank's requirement.	Additional clause not accepted.
129	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc.	The solution should support Monitoring Mode and blocking Mode of Deployment. In monitoring mode, solution can generate alerts for unauthorized activity. In blocking mode, solution must proactively block the queries including blocking of matching signatures for known attacks like SQL injection.	Additional clause not accepted.
130	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc.	The solution should be capable of blocking access, real time execution of commands which violates the rule/ policies, store the events securely and report the same in real time.	Additional clause not accepted.
131	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	Provides real-time database protection against internal and external threats by alerting or blocking attacks and abnormal access requests. Solution should provide virtual patching for a number of database software vulnerabilities, reducing the window of	Additional clause not accepted.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					exposure and impact of long patch cycles.	
132	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should have automated DB profile in the totality of all the user profiles for the DB application's users and a policy can be rendered around the profile	Additional clause not accepted.
133	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	Solution should have dynamic profiling capability to automatically examine traffic for creation of comprehensive profiling of database structure and behavior.	Additional clause not accepted.
134	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should support the following database types but not limited to: 1. Conventional Databases 2. In-Memory databases 3. Application in-build databases 4. Big Database types 5. Data lakes 6. Cloud based databases	Additional clause not accepted.
135	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The Bank should be able to deploy or remove the proposed solution from the network with no impact on the existing databases or the network architecture.	Additional clause not accepted.
136	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should be scalable and support all types of storage but not limited to, such as DAS/NAS & SAN for increasing audit storage.	Additional clause not accepted.
137	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should support automatic updates to the signature database and based on global threat intelligence, regulatory and non- regulatory	Additional clause not accepted.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					standards, ensuring complete protection against the latest threats.	
138	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should support custom security rules. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.	Additional clause not accepted.
139	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should allow policy definitions using very granular parameter like and not limited to: date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. and should offer to input any policy exceptions	Additional clause not accepted.
140	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should have the ability to generate report showing the access of each user to the tables of each database along with the user who granted them the permission.	Additional clause not accepted.
141	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.	Additional clause not accepted.
142	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution should provide a capability to enforce policies based on the compliance- controlled database [Like PCI complied databases apply CC transaction and retrieval policy violations], group of databases, Database types [Oracle and MS SQL	Additional clause not accepted.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					specific policies, locations [GDPR policies for all DB's hosted in EU], User Specific Polices"	
143	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution must support generation/both predefined as well as custom built reports as per customer requirements with both tabular views, pdf and data analysis graphical views, etc. The solution should be able to generate the reports in PDF, Excel & CSV formats, etc.	Additional clause not accepted.
144	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Requesting Bank to add additional clauses as these are mandatory clauses asked by Auditors such as RBI, SEBI, PCI etc	The solution must be able to support the identification of anomalous activity based on DAM monitoring and control for the following databases but not limited to, - MSSQL - Oracle - CASSANDRA -Hadoop -PostgreSQL -MySQL -MongoDB, etc.	Additional clause not accepted.
145	Annexure 10	Sheet 4 (DAM)	Functional & Technical Requirement	Additional Clause	User rights management for databases enables automatic aggregation and review of user access rights. Solution should identify more privileges rights and dormant users based on Bank context and actual usage. The solution should enable bank to demonstrate compliance with regulations such as	Additional clause not accepted.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					regulatory/Govt guidelines received from time to time, ISO 27701 (ISO 27000 family), PCIDSS and reduce the risk of data breach.	
146	Annexture 10				To size the solution appropriately it's important to understand the current Network throughput capacity Kindly provide the clarity on this.	Current Network throughput is around 750 Mbps.
147	Annexture 10				Please confirm if we need to consider all three location -DC, DR, and NDR - When sizing the solution. Additionally, is local HA required at each site?	The Bidder shall consider implementation of bank-end CSOC components at Bank's DC (in HA mode) & DR (In Standalone mode) only. CSOC should monitor entire Bank's infrastructure including the NDR.
148	Annexture 10		1.3 (Basic requirement)	Proposed NBAD systems should have adequate inbuilt storage for retaining minimum 30 days data from day 1.	Please provide clarity on the retention period for 1. Metadata 2. Raw data	Both the data should be stored for given period.
149	Annexture 10		2.3 (Visibility and identity awareness)	The Solution should be able to detect Malwares on both encrypted and nonencrypted payloads.	To detect malware within a payload, full packet capture is essential as payload extraction cannot be performed using Netflow. Please ensure that clause number 3 from the additional points is included. Additionally, it's important to note that traffic/payload decryption is a function of SSLO. NBAD is capable of detecting malicious objects and malware payloads in plaintext traffic provided by SSLO. Kindly adjust the clause accordingly.	RFP Requirement stands. Please refer existing solutions available with Bank
150	Annexture 10		3.13 (Functional requirements)	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	NSEL is Cisco proprietary, kindly delete this from this clause . Kindly add full packet capture to comply with the clause 4.25 & 4.14 , therefore rephrase it to " The solution should support all	Revised Clause: The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd and full packet capture.	
151	Annexture 10		3 (Functional requirements)	Request you to add this specification in your RFP requirement	The solution should be a dedicated behavior analytics solution delivering advanced Network detection and Response (NBAD/NDR) use cases and not a subset capability of SIEM and SOAR.	Clause not considered
152	Annexture 10		3 (Functional requirements)	Request you to add this specification in your RFP requirement	The solution must include a built-in, fully functional capability similar to Wireshark, allowing users to view and analyze event sequences using PCAP files without relying on any third-party tools.	Clause not considered
153	Annexture 10		3 (Functional requirements)	Request you to add this specification in your RFP requirement	The solution should capture and record all network packets in full (both header and payload) by ingesting raw traffic to provide comprehensive visibility upto layer 7 for detailed threat detection and application aware security to ensure early identification and mitigation of advanced network- borne threats. Additinaly should be able to retain Full packet for 5 days and metadata for 180 days.	Clause not considered
154	Annexture 10		4.9 (Threat detection capability)	The solution must detect unusual, unauthorized behavior within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, unauthorized use of access credentials to internal resources.	This is a NAC feature and not a NBAD feature. NBAD doesn't know if the device or access credential is authorized or unauthorized.Kindly delete this clause from NBAD's specifications.	Please consider the clause as deleted

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
155	Annexture 10		4.0 (Threat detection capability)	Request you to add this specification in your RFP requirement	The solution should provide an integrated Malware analysis engine to emulate malware or any unknown malicious object, file etc. seen in the network communication to provide defense against advanced and sophisticated network-borne threats.	Clause not considered
156	Annexture 10		4.37 (Threat detection capability)	The solution must be able to provide visibility of user endpoint workstations and support & service options to collect telemetry from these endpoints including username, process names and process hashes involved in the network traffic.	NBAD as the name suggests is a network monitoring solution and does not have any endpoint agents. These agents are typically under the scope of either NAC or EDR. The following provides all the details which can be captured looking at the network traffic such as IP Address, MAC Address, Port no, Application used, etc. However process names and hashes are under the scope of agent based technologies such as EDR and NAC. Hence request you to kindly rephrase the clause.	Revised Clause: The solution must be able to provide visibility of user endpoint workstations network traffic.
157	Annexture 10		5.3 (Integration)	The solution must integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, Router, Switches, NAC, Proxy, WAF, mail gateway etc. Necessary applicable licenses for integration with other security devices must be supplied from day one.	Kindly rephrase this clause as "The solution must integrate with existing security solutions like Security Information and Event Management (SIEM), Next-generation Firewalls, and Router, Switches, Proxy, WAF, mail gateway for packet data. Necessary applicable licenses for integration with other security devices must be supplied from day one."	RFP Requirement stands
158	Annexture 10		7.7 (Management)	The solution should have an automated scanner to identify assets and should also be able to schedule the scans	This is a feature of Vulnerability scanner. Kindly delete this clause from NBAD's specifications.	Please consider the clause as deleted

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
159	Annexture 10		8.1 (The solution should allow custom dynamic dashboard creation)	The solution should have detailed ASN traffic visibility	This is an OEM specific clause, kindly delete this clause for the wider participation of other OEM's	Please consider the clause as deleted
160	Annexture 10		8.4 (The solution should allow custom dynamic dashboard creation)	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds	This is an OEM specific clause, kindly delete this clause for the wider participation of other OEM's	Please consider the clause as deleted
161	Annexture 10		NBAD: Point 8.2	The solution should have native integration with any PDNS service to obtain unlimited DNS resolution and domains hosted information along with WHOIS directly from the portal	This is an OEM specific clause, kindly delete this clause for the wider participation of other OEM's	Please consider the clause as deleted
162			Excel Spreadsheet for SOAR - Sl. No. 3	SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner	We Request you to kindly amend the clause as: SOAR solution should collect real time global threat intel data, dedupe and process threat intelligence in a holistic and actionable manner	Revised Clause: SOAR solution should collect real time global threat intel data, dedupe and process threat intelligence in a holistic and actionable manner.
163			Excel Spreadsheet for SOAR - Sl. No. 5	The solution should provide option to manually invoke selected playbook based on any selected or set of selected events.	The solution should provide option to manually invoke the playbook based on pre-defined criteria's based on any selected incident.	RFP Requirement Stands
164			Excel Spreadsheet for SOAR - Sl. No. 27	Solution should support grouping of multiple incidents of similar type into one incident	Solution should be able to co-relate and show relationships between various incidents	RFP Requirement Stands
165			Excel Spreadsheet for SOAR - Sl. No. 28	Solution must maintain repository of IOCs which can be associated with any stage of a cyber kill chain for an incident.	Solution must maintain repository of IOCs which can be associated with MITRE ATT&CK Framework for an incident.	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
166	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	Solution should strengthen end point security solution with improved visibility and new technical controls to detect and prevent from advanced sophisticated attack against users including Anti Phishing , Web form protection, account takeover protection, Browser based attacks and corporate credential theft.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	Revised clause: Solution should strengthen end point security solution with improved visibility and new technical controls to detect and prevent from advanced sophisticated attacks, Browser based attacks and corporate credential theft.
167	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	Revised clause: Solution must detect and block access to phishing sites. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's
168	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	Solution should have protection for account takeover attacks and also solution should alert users on the reuse of corporate password use on external sites	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	Revised clause: Solution should alert users on the reuse of corporate password use on external sites
169	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	Solution should have capability to detect and prevent different exploit techniques including ROP chaining , ASLR Bypass , VBScript God Mode , Stack Pivoting and BlueKeep without having signature database.	Kindly rephrase as " Solution should have capability to detect and prevent different exploit techniques"	Revised Clause: Solution should have capability to detect and prevent different exploit techniques.
170	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	Solution should not have dependency on 3rd party ssl interceptor and also does not require any additional client certificate to inspect ssl traffic at browser level. The solution must have inbuilt ransomware detection mechanism. The solution must be able to identify 0-day attacks, emulate the threat while eliminating the threat on a	Kindly rephrase as "The solution must have inbuilt ransomware detection mechanism, along with rollback remediation capability incase of ransomware attacks. The solution must be able to identify 0-day attacks."	Revised Clause: The solution must have inbuilt ransomware detection mechanism. The solution must be able to identify 0-day attacks.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				real-time basis and deliver the file to the user by reconstructing the content.		
171	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The Solution should have interface to search for IOCs provided through the endpoint management UI, CLI and an API. The search will return a list of all endpoints which match the IOCs	kindly remove CLI and API for maximum participation.	Revised clause: The Solution should have interface to search for IOCs provided through the endpoint management UI. The search will return a list of all endpoints which match the IOCs
172	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on both monitored and non-monitored systems.	Requesting to Kindly amend this point for maximum participation as "The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on managed systems"	Revised Clause: The solution should be able to take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. The admin should be able to capture snapshots on monitored systems.
173	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to show files read, moved, executed, modified, deleted and attribute changed on a particular device in a particular time frame.	The above statement isn’t a part of EDR solution. Kindly request to remove the statement for maximum participation	RFP Requirement Stands
174	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to show Network Connections, Service Changed, Admin/Hacking tools, Script Written and DNS requests made by the device in a particular time frame	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	RFP Requirement Stands
175	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to show lists the DLLs that are loaded by processes and lists the activities performed by Windows Management Instrumentation (WMI) service on a particular device in a particular time frame.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	RFP Requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
176	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should collect Browser Download information including file downloaded, URL from where file was downloaded, size of file, user profile and when download started.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	RFP Requirement Stands
177	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should collect Browser History information including URL visited, last visit time, visit count and browser used.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	Revised Clause: The solution should collect Browser History information including URL visited, last visit time and browser used.
178	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should collect file information including file name, directory path, File size, md5, DES-3 and sha1 hash, time of creation and deletion and user executing the process.	Kindly amend as " The solution should collect file information including file name, directory path, File size, md5, DES-3 and sha1 hash and user executing the process." for maximum participation	Revised Clause: The solution should collect file information including file name, directory path, File size, md5, DES-3, AES, sha256 and sha1 hash and user executing the process.
179	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution collect information regarding services installed on managed devices including service name, start-up mode, current status of the service and user that owns the service's process.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	RFP Requirement Stands
180	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to provide historic user logon activity for a particular endpoint in a specific time frame.	The given statement is not related to endpoint security and only favoring a specific vendor. Kindly remove this point for maximum participation.	RFP Requirement Stands
181	Annexure 10 Functional and Technical Requriement. xls		End Point Detection and Response (EDR)	The solution should be able to run a vulnerability scan on a particular endpoint if under investigation.	The given statement is favoring to specific vendor. Requesting you to kindly remove this point for maximum participation	Please consider the clause as deleted

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
182	Annexure 10 functional and technical requirement – PIM			Bidder must consider to deploy the solution for supporting minimum 50 User License from day one in Bank, DC(standalone), DR(standalone) and NDR (standalone)	Our License model is based on the Number of Privilege password Administrators and SSH keys stored within the PIM/PAM Solution – Can you let us know the total number of password administrators and total number of SSH keys required to be stored in the Solution .	The Bidder shall consider implementation of bank-end CSOC components at Bank's DC (in HA mode) & DR (In Standalone mode) only. CSOC should monitor entire Bank's infrastructure including the NDR.
183	Annexure 10 functional and technical requirement – PIM			Multifactor Authentication (MFA) : Solution supports integrated Multifactor including soft token via SMS, Email, time tokens via mobile application or mobile push authentication	Apart from SMS we can support other mechanisms, Need to be modified as "Multifactor Authentication (MFA) : Solution supports integrated Multifactor including soft token via Email, time tokens via mobile application or mobile push authentication"	RFP requirement stands
184	Annexure 10 functional and technical requirement – SIEM			Bidder must consider to deploy the solution for supporting minimum 700 assets or upto 5000 EPS from day one in Bank, DC(HA) and DR(standalone), NDR	Need modification over the clause as the solution supports DC and DR, "Bidder must consider to deploy the solution for supporting minimum 700 assets or upto 5000 EPS from day one in Bank, DC(HA) and DR(standalone)"	The Bidder shall consider implementation of bank-end CSOC components at Bank's DC (in HA mode) & DR (In Standalone mode) only. CSOC should monitor entire Bank's infrastructure including the NDR.
185	Annexure 10 functional and technical requirement – SIEM			Bidder must consider to deploy the solution for supporting minimum 700 assets or upto 5000 EPS from day one in Bank, DC(HA) and DR(standalone), NDR	Need more information on the split of the overall 700 Devices mentioned : Do we have multi site or all the devices are present in the single location ? Number of windows Servers Number of Windows Workstation Number of Syslog devices (syslog device could be a Router, Switch, Firewall, IDS/IPS, IBM AS 400 Machine, Linux or Unix Systems or any Syslog Sources.) : Number of Domain Controllers in case of On Prem AD : Number of File Servers: Number of Linux Servers: Number NetApp/EMC/Synology Nas : Number	Kindly refer RFP Clause No.2.1 The Bidder is expected to do following but not limited to, Table "Assets to be integrated for CSOC: "for detail information.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					of MS SQL Servers: Number of IIS Sites: Number of O365 Tenants: Number of AWS Account: Number of Exchange Servers: Number of Other application sources with syslog forwarding capabilities:	
186					Request for Clarification: In Part 2 Bank is asking for, *"Bank expects below solutions to be provided as part of SOC, but the management & monitoring will cover all devices & solutions implemented at bank's end"* Our Understanding: The proposed solutions that needs to be deployed in PDCC as pe "Annexure 11 Commercial Bill of Material" will be under Bidder will be under bidder Scope only	Understanding is correct

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
187	Additional Query			Additional Query	Request for Clarification: Is PDDC looking 24/7/365 Device Management for DC Data Center, DR Site, NDR, HO, Branches and Service Outlets and for the hardware/software applications of the PDCC Bank? As we can clearly see the Annexure 11 Commercial Bill of Material is only asking for the cost for software licenses, CSOC monitoring support and ATS of the proposed solution shared in that specific list of solutions as mentioned in RFP page no. 9 detailed scope of work. • Network Access Control (NAC), • Endpoint Detection Response (EDR), • Endpoint Forensic and Behavior Analysis (EFBA), • Database activity monitoring (DAM), • Security information and event management (SIEM) (as service), • Privileged identity and Access management (PIM/PAM), • Network Behavior Anomaly Detection (NBAD), • Threat Intelligence (as service), • SOAR (as service), • VAPT tool as per NABARD guidelines, • Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge etc. (as service). • Dark web monitoring s(as service)	24*7*365 Monitoring of the proposed Hardware, applications and services should be provided by bidder.

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
188	Additional Clause			Termination for default	We propose to add new clause: Termination for default: Bidder if in case the Bank has materially breached any terms and conditions of the the contract, shall inform Bank of the same through a notice in writing giving thirty (30) days' time for remedying the breach. The bidder may terminate the contract, if such breach is not remedied during such thirty (30) day period.	Additional clause not accepted
189	Additional Clause			Non-solicitation of employees (addition of new clause)	We propose to add below mention clause : During the term of this Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s or subcontractor/s of the other Party, or aid any third person to do so, without the specific written consent of the other Party. This restriction shall not apply to employees of either Party responding to advertisements in job fairs or news media circulated to the general public.	Additional clause not accepted
190				Network Switches	Please confirm if bidder need to supply the network switches in DC, DR and NDR location?, if yes, what is the uplink	Not required
191					Do you need the NDR configuration same as DR or can NDR be at a reduced capacity.	Kindly refer RFP Clause No.2.1 The Bidder is expected to do following but not limited to, Table "Assets to be integrated for CSOC: "for detail information. NDR will not have any CSOC

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
						components implemented but NDR's devices shall be monitored through CSOC.
192	General Query			Vulnerability Assessment & Penetration Testing tool for critical devices/ servers /applications/ solutions.	What are the total number of devices considered for Vulnerability Management?	It will be discussed with Final selected bidder.
193	General Query			Vulnerability Assessment & Penetration Testing tool for critical devices/ servers /applications/ solutions.	What will be the frequency of scans	Kindly refer RFP Clause No.2.1 The Bidder is expected to do following but not limited to, Point no. 27 for detail information.
194	General Query			Vulnerability Assessment & Penetration Testing tool for critical devices/ servers /applications/ solutions.	What will be the frequency for Penetration Testing?	Kindly refer RFP Clause No.2.1 The Bidder is expected to do following but not limited to, Point no. 27 for detail information.
195	General Query			Vulnerability Assessment & Penetration Testing tool for critical devices/ servers /applications/ solutions.	What will be the total number of assets considered for Penetration Testing?	It will be discussed with Final selected bidder.
196	General Query			Vulnerability Assessment & Penetration Testing tool for critical devices/ servers /applications/ solutions.	Is configuration Audit also in scope?	It will be discussed with Final selected bidder.
197	6.23 - Patent right	40	6.23 - Patent right	In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the Goods or any part thereof in India, the Bidder shall act expeditiously to extinguish such claims. If the Bidder fails to comply and PDCC Bank is required to pay compensation to a third party resulting from such infringement, the Bidder shall be responsible for the compensation including all expenses, court costs and lawyer fees. PDCC Bank will give notice to the Bidder of such claims, if it is made, without delay.	Legal Comment: We cannot accept the original indemnity clause as it imposes broad and potentially burdensome liability on the Bidder for all third-party intellectual property claims, including international claims. This extensive obligation could lead to significant financial and operational risks, particularly given the complexity of managing such claims. We propose the revised clause, which balances the intent of indemnity with a more manageable approach "In the event of a third-party claim of intellectual property infringement, the	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				PDCC Bank will give notice to the Bidder of any such claim without delay, provide reasonable assistance to the Bidder in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.	Bidder may, at its sole discretion, (i) secure the right for PDCC Bank to continue using the Goods or Software, (ii) modify the Goods or Software to eliminate the infringement, (iii) replace the Goods or Software with a functionally equivalent, non-infringing alternative, or (iv) if the options in (i)-(iii) are not feasible, notify PDCC Bank and terminate the infringing Goods or Software without penalty to either party. The Bidder shall also indemnify PDCC Bank against any costs, damages, or expenses incurred due to such claims, including reasonable legal fees, provided that PDCC Bank promptly notifies the Bidder of any such claim and cooperates in resolving it. This indemnity obligation is limited to the remedies described herein and constitutes PDCC Bank's sole remedy for intellectual property infringement claims.	
198	6.21	39	6.21 Indemnity	6.21 Indemnity Bidder hereby indemnifies the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, (hereinafter collectively referred to as 'Personnel") 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	Legal Comment: We cannot accept the indemnity clause as it currently stands because it places an unfair burden on us. It requires us to cover a wide range of risks, including issues caused by the Bank's authorized use of our deliverables, and holds us liable for third-party claims beyond our control. Additionally, the clause does not limit our liability for infringement or financial losses related to issues caused by the Bank's instructions or modifications. We insist on revising the clause to	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				proceeding brought against the Bank by a third Party as a result of: 1. The Bank authorized / bona fide use of the deliverables and /or the Services provided by Bidder under this Agreement; and/or 2. An act or omission of the Bidder, employees, agents, subcontractors in the performance of the obligations of the Bidder under this Agreement; and/or 3. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder against the Bank; and/or 4. any or all deliverables or services infringing any patent, trademarks, copyrights or such other IPR; and/or 5. Breach of confidentiality obligations of Bidder contained in this agreement; and/or 6. Negligence or gross misconduct attributable to the Bidder or its employees or sub-contractors Bidder at its own cost and expenses defend or settle any claim against the bank that the deliverables and services delivered or provided under this agreement infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trademark in the country where the Deliverables and Services are used, sold or received, provided the Bank: a. Notifies the Bidder in writing; and	introduce mutual responsibilities and more balanced risk-sharing. Proposed clause: Each Party shall indemnify, defend, and hold the other Party, including its employees, personnel, officers, and directors (collectively, "Personnel"), harmless from and against any claims by third parties (including any Governmental Authority), and related expenses (including legal fees and court costs), arising from damage to tangible property, personal injury, or death caused by such Party’s negligence or willful misconduct. The Bank shall also indemnify, defend, and hold the Bidder harmless from any and all claims (including claims by any Governmental Authority seeking to impose penalties or criminal sanctions) arising from: The Bank’s or its end users’ use of the deliverables and/or services provided under this Agreement; and/or The Bank’s breach of confidentiality obligations, intellectual property rights, or any other material obligations under this Agreement. This indemnity is subject to the conditions that the indemnified Party: a. Notifies the indemnifying Party in writing promptly upon learning of any claim; b. Cooperates with the	

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				b. Co-operates with the Bidder in the defence and settlement of the claims. Notwithstanding the above, Bidder shall not have any liability to Bank under this Section to the extent that any infringement or claim thereof is attributable to: a. The combination, operation or use of a Deliverable with equipment or software supplied by Bank where the Deliverable would not itself be infringing. b. Compliance with designs, specifications or instructions provided by Bank. c. Use of a Deliverable in an application or environment for which it was not designed or contemplated under this Agreement; or d. Modifications of a Deliverable by anyone other than Bidder where the unmodified version of the Deliverable would not have been infringing. Bidder will completely satisfy its obligations hereunder if, after receiving notice of a claim, Bidder obtains for Bank the right to continue using such Deliverables as provided without infringement or replace or modify such Deliverables so that they become no infringing. Bidder shall compensate the Bank for financial loss, suffered by the Bank if the Bidder fails to fix bugs, provide the modifications / enhancements / customization as required by the Bank as per the terms and conditions of this	indemnifying Party in defending or settling the claim; and c. Does not make any admissions or settlements without the indemnifying Party's prior written consent.	

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				Agreement and to meet the service levels. The Bank hereby indemnifies the Bidder, and shall always keep indemnified and hold the Bidder harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including reasonable attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought by third parties against the Bidder as a result of: a. Third party infringement claims resulting from unauthorized equipment modification by the Bank or equipment use prohibited by specifications for hardware and Software. b.Third-party infringement claims resulting from a breach of Software license terms taken by the Bidder in respect of services provided by the Bidder. c. Bidder shall not be liable for defects or nonconformance resulting from unauthorized modification, use or operation of core banking suite of software by bank.		
199	6.30	42	6.30 Effect of Termination	6.30 Effect of Termination Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment. Reverse Transition mechanism would typically include service and tasks that	Legal Comment : We cannot accept this clause as it imposes indefinite obligations post-contract, mandates the same payment terms despite potential cost changes, and requires continued maintenance services without fair compensation. Additionally, it allows the Bank to	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				are required to be performed / rendered by Bidder to PDCC Bank or its designee to ensure smooth handover (including data) and transitioning of PDCC Bank's deliverables, maintenance, removal of PDCC Bank's all data from the system/ cloud and facility management. Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services. The reverse transition phase shall be completed within 3 months. Bidder agrees that after completion of the Term or upon earlier termination of the assignment Bidder shall, if required by PDCC Bank, continue to provide maintenance services to PDCC Bank at no less favorable terms than those contained in this document. In case PDCC Bank wants to continue with Bidder's services after the completion of this contract then Bidder shall offer the same or better terms to PDCC Bank. Unless mutually agreed, the rates shall remain firm. Bidder agrees that PDCC Bank at any point of time during tenure of contract may return/discontinue any of the Deliverables/services in whole or part thereof offered under this document. PDCC Bank shall not be liable to make any payment in respect of the Deliverables/services returned in whole or part thereof.	unilaterally discontinue services without liability, creating financial risk for the bidder. We recommend revising the clause to ensure a fairer and more balanced arrangement. Proposed Clause: Upon termination or expiration of the contract, the Bidder agrees to provide reverse transition services to PDCC Bank or its designee for a smooth handover, including data transfer and transitioning of deliverables. This will be done under mutually agreed terms and conditions, including fair compensation for the Bidder, based on the complexity and scope of the reverse transition tasks. Both parties agree to negotiate the reverse transition phase, which shall not exceed three months unless mutually extended. During this period, the terms (including payment terms) applicable during the contract may be reviewed and adjusted to reflect any changes in market conditions or resource requirements. Should PDCC Bank wish to continue with the Bidder's services post-contract, both parties will negotiate new terms, including rates and conditions, based on prevailing circumstances. Any continued maintenance services provided by the Bidder after the contract term will also	

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					be subject to mutually agreed terms, ensuring fair compensation. PDCC Bank reserves the right to return or discontinue any deliverables or services under this contract, but the Bank will be liable for any costs incurred by the Bidder up until the point of discontinuation, ensuring that the Bidder is fairly compensated for resources and efforts already committed.	
200	6.29	42	6.29 Termination for Convenience	6.29 Termination for Convenience PDCC Bank, by written notice sent to Bidder, may terminate the Contract with a notice of 3 months, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for PDCC Bank's convenience, the extent to which performance of work under the Contract is terminated and the date upon which such termination becomes effective.	Legal Comment: We cannot accept this clause as it allows the Bank to unilaterally terminate the contract at any time for convenience, without ensuring fair compensation for the bidder's committed resources, efforts, and costs. This creates financial uncertainty and risk for the bidder. Proposed Clause: Either party may terminate the contract, in whole or in part, for convenience by providing the other party with a minimum of three months' written notice. In the event of termination for convenience by PDCC Bank, the Bank shall compensate the Bidder for all reasonable costs, expenses, and non-cancellable commitments incurred up to the termination date. The Bidder shall not be liable to pay any compensation to PDCC Bank upon termination for convenience.	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
201	6.31	42	6.31	6.31 Renewal of Contract In case PDCC Bank wants to continue with Bidder's services after the completion of this contract, Bidder shall offer the same services or enhanced services to PDCC Bank. Unless mutually agreed, the same rates shall apply.	Legal Comment: We cannot accept this clause as it obligates the bidder to offer the same or enhanced services at the same rates post-contract, without considering potential changes in costs, market conditions, or service scope. This limits the bidder's ability to adjust pricing and terms fairly. Proposed Clause: If PDCC Bank wishes to continue with the Bidder's services after the completion of this contract, both parties shall negotiate the terms and conditions of the renewal, including any adjustments to service scope, rates, and conditions, based on prevailing market factors and mutual agreement. Any renewal shall be subject to mutual consent in writing	RFP requirement Stands
202	6.37	46	6.37	6.37 Bidders Liability Bidder's aggregate liability in connection with obligations undertaken as a part of this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the total value of the contract under this Agreement. However, Bidder's liability in case of claims against the Bank resulting from misconduct or gross negligence of the Bidder, its employees and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or	Legal Comment: We cannot accept this clause as it imposes unlimited liability for claims related to misconduct, gross negligence, or intellectual property infringement. Additionally, it does not exclude liability for indirect, special, consequential, or incidental damages, which can result in disproportionate financial exposure for the bidder. Proposed Clause: The Bidder's aggregate liability in connection with obligations undertaken as part of this project, regardless of the form or nature of the action (whether in contract, tort, or otherwise), shall be limited to the total value of the contract	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
				breach of confidentiality obligations will not be limited. The Bank including its promoters, directors, executives and employees shall not be held liable for and are absolved of any responsibility or claim litigation arising out of the use of any third-party software or modules supplied by the Bidder.	under this Agreement. The Bidder shall not be liable for any indirect, special, consequential, or incidental damages, including loss of profits or revenue. However, the Bidder's liability in cases of claims resulting from its gross negligence, willful misconduct, or infringement of patents, trademarks, copyrights, or other intellectual property rights, as well as breaches of confidentiality obligations, shall be limited to direct damages and capped at the total contract value. The Bank, including its promoters, directors, executives, and employees, shall not be held liable for any claims or litigation arising from the use of any third-party software or modules supplied by the Bidder.	
203	41	15	41	The proposed solution by Bidder will be 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. Bidder shall provide assistance during cyber security drills / audits as and when conducted without any additional costs.	The audit rights can only be provided to the extent of the scope of work, and notice of audit is also required to be given to the Bidder. Proposed Clause: The Bank shall have the right to audit the Bidder's performance under this Agreement, but only to the extent necessary to verify compliance with the scope of work outlined in this contract. The Bank agrees to provide the Bidder with a written notice of at least 15 business days prior to any audit. Such audits shall be conducted during normal business	RFP requirement Stands

Sr. No	Section Number	Page Number	Point Number	Original Clause	Query	PDCC Bank Response
					hours, and the Bank shall ensure that the audit process is reasonable and does not unduly interfere with the Bidder's operations. Any audit shall be limited to the records and documents directly related to the services provided under this Agreement.	