தமிழ்நாடு கிராம வங்கி
TAMIL NADU GRAMA BANK
(A Government owned Bank Sponsored by Indian Bank)

Amendments to the RFP No:TMD/10/2023-24 dated 04/09/2023

S.No	Page No	Clause Name	Existing RFP Clause	Amended RFP Clause
1	9	Pre-qualification CSOC Setup	a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.	a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2022 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) The bidder should have experience in implementing the make of solution proposed for this tender for other clients of the bidder. However it is not required that SIEM, WAF and EDR must be of same OEM
2	10	Pre Qualification Criteria	3.9 The bidder should have captive SOC in their premises live from or before 31 Mar 2020 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.	3.9 The bidder should have captive SOC in their premises and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.
3	11	Man Power	Each L2 resource should have certification in 2 or more solutions	Out of three L2 resources, One L2 resource should be certified in two or more solutions from group 1, second L2 should be certified in two or more solutions from group 2 and third L2 should be certified in two or more solutions from group 3 from three groups mentioned in page no 24 and 25 of the RFP.

4	20	Payment Terms	Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources 50 % of [A]-Device Cost 50% of [E]-License Cost	Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources 70 % of [A]-Device Cost 70% of [E]-License Cost
5	20	Payment Terms	Post successful Implementation and after Signoff. 50 % of [A] 50% of [B] 50% of [E]	Post successful Implementation and after Signoff. 30 % of [A] 50% of [B] 30% of [E]
6	23	SERVICE LEVEL AGREEMENT (SLA)	The applicable penalties would be the same irrespective of the root cause.	The applicable penalties would be the same irrespective of the root cause if the delay/downtime is attributable to the successful bidder.
7	24	Hardware / Solution Uptime	Hardware / Solution Uptime - Group I Minimum 99.99% of uptime to be maintained.	For Web Proxy with DLP, Minimum 99.95% of uptime to be maintained. For other solutions in Group 1, mininum 99.99% of uptime to be maintained. Deduction below minimum uptime will attract SLA penalty. Uptime will be calculated on monthly basis.
8	27	Penalty	b) Penalty due to absence of any engineer in one quarter will be capped at 100% of the Quarterly FM amount for that resource.	b) Penalty due to absence of any engineer in one quarter will be capped at 120% of the Quarterly FM amount for that resource. For L2 resources, leave for 12 days in a year are permitted.
9	30	Price after contract	If the contract is extended for any period, beyond its expiry, the prices shall remain fixed as per the contract signed between the Bank and the Bidder, regardless of variation of exchange rate.	If the contract is extended for any period, beyond its expiry, the prices shall be fixed as per mutually agreed terms between the Bank and the Bidder. However variation of exchange rate will not be considered.
10	36	WAF	Bidder to provide new WAF devices with latest features (two at DC) and (One at DRS) as per technical specifications.	Bidder to provide new WAF devices with latest features (two at DC) and (two at DRS) as per technical specifications.

11	37	PIM	Additional Clause	Existing configuration and rule set to be reviewed and addition / modification has to be done in consultation with the bank
12	38	Scope of work	Bidder has to develop and maintain Standard Operating Procedures (SOP) for the day to day operations of all the solutions to be managed by the Bidder. The SOPs should cover at least vulnerability/ threat management, alert/incident management, rules creation & fine tuning, installation/upgradation, signed firmware updates, asset Integration, Business Continuity data & configuration backup, restoration testing, archival, knowledge management, segregation of duties, change management, patch & version management, as per policies of the Bank for all the applications including databases in the scope. Bidder is expected to create and modify SOPs as per the requirement of the Bank periodically and from time to time, as applicable.	Bidder has to develop and maintain Standard Operating Procedures (SOP) for the day to day operations of all the solutions to be managed by the Bidder. The SOPs should cover at least vulnerability/ threat management, alert/incident management, rules creation & fine tuning, installation/upgradation, signed firmware updates, asset Integration, Business Continuity data & configuration backup, restoration testing, archival, knowledge management, segregation of duties, change management, patch & version management, as per policies of the Bank for all the applications including databases in the scope. Bidder is expected to create and modify SOPs as per the requirement of the Bank periodically and from time to time, as applicable; Configuration and rule changes has to be incorporated.
13	38	Scope of work	Bidder has to provide reports for all the solutions on a daily basis for executive reporting in addition to the detailed reports. Some of the reports may be required multiple times in a day. Bank may also ask customised reports of any solution based on Bank's requirement and same has to be provided.	Bidder has to provide reports for all the solutions on a daily, weekly and monthly basis for executive reporting in addition to the detailed reports. Some of the reports may be required multiple times in a day. Bank may also ask customised reports of any solution based on Bank's requirement and same has to be provided.
14	39	SCOPE OF WORK	Only after successful running of solutions for one-month period, the solutions will be taken over by successful bidder's facility management/ onsite support engineers for providing further services as per scope of work of this RFP document	The solutions will be taken over by successful bidder's facility management/ onsite support engineers for operations after the implementation and sign off as per scope of work of this RFP document
15	39	Scope of work	The Bidder should ensure agent upgradation as per OEM recommendation within the timeline stipulated by the Bank for all the applicable solutions. The agent should be deployed/installed/redeployed/upgraded using bidder's supplied solution without any need to have dependency on any other solution in the Bank	The Bidder should ensure agent upgradation as per OEM recommendation within the timeline stipulated by the Bank for all the applicable solutions. The agent should be deployed/installed/redeployed/upgraded using bidder's supplied solution without any need to have dependency on

				any other solution in the Bank ; Appropriate On the job training has to be provided to the team concerned
16	39	Scope of work	There should be a provision of adequate Business Continuity Plan (BCP) for all the Cyber Security Solutions (new Cyber Security Solutions as well as existing security solutions as per Scope mentioned in this RFP).	There should be a provision of adequate Business Continuity Plan (BCP) for all the Cyber Security Solutions (new Cyber Security Solutions as well as existing security solutions as per Scope mentioned in this RFP). All technologies should have arrangement for disaster recovery systems available.
17	41	Requirement of Man power	e) The successful Bidder has to deploy additional manpower, without any additional cost to the Bank, so as to substitute the off-day, weekly-off, holiday, compensatory off and leave of the L1 resources. Bank will be liable to pay only for the number of resources as mentioned in this RFP or as per the Purchase Order. Further, penalty for the shortfall of Manpower deployed will be levied which will be additional 20% above the deduction of absence of resources. For L2 resources, leave for 12 days in a year are permitted.	Clause deleted
18	44	Requirement of Man power	B.E. /B.Tech or above in Computer Science/Electronics/IT/Electrical Engineering/ MCA.	B.E. /B.Tech or above in Computer Science/Electronics/IT/Electrical Engineering.
19	44	Man Power	Position: Level-1 (L1) BSc /Diploma or above in Computer Science/Electronics/IT/Electrical Engineering.	Position: Level-1 (L1) B.E/B.Tech or above in Computer Science/Computer Applications/Electronics/IT/Electrical Engineering.
20	46	Delivery timelines	Additional Clause	For delivery of softwares, delivery instructions shall be issued by the bank post signing of the contract within three months from start of contract.

21	50	Internal Firewall	The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	The other physical ports should be- atleast 8 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+
22	54	External Firewall	The throughput of the Firewall solution should be minimum 1 Gbps after enabling NIPS, Anti-APT, sandboxing, Logging etc. with recommended secured algorithms during the contract period.	Clause deleted
23	54	External Firewall	Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput	Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput(after enabling NIPS, Anti-APT, sandboxing, Logging etc)
24	57	External Firewall	Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1	Clause deleted
25	57	External Firewall	Appliance must have minimum 32 GB of RAM, minimum 12 physical cores and 240 GB storage. RAM Should be upgradable up to 128 GB	Clause deleted
26	61	SIEM	The proposed solution should be sized for 5,000 sustained EPS at correlation layer initially per Data centre but should be able to handle peak >License deployed EPS (additional 5000 EPS to take care of spikes/ burst / outbreak / flood in traffic) at correlation layer without dropping events or queuing events (for SIEM) per Data Centre.	The proposed solution should be sized for 5,000 sustained EPS at correlation layer initially at Data centre

27	65	SIEM	"The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier."	"The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier.This specification is not mandatory for Make in India products".
28	66	SIEM	"SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.)"	"SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.) This specification is not mandatory for Make in India products".
29	67	WAF	The WAF Appliance must be a dedicated hardware and it should not be clubbed with Load Balancers/ADC	The WAF Appliance must be a dedicated hardware with inbuilt load balancer
30	67	Hardware/WAF	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure.	Clause deleted
31	68	WAF	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.	The solution must support the configuration to allow some applications to be in detection / learning mode and some applications in blocking mode.
32	69	WAF	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Clause deleted

33	73	WAF	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	Clause deleted
34	73	WAF	The Solution should also have a runtime plugin that would get installed on the Application Servers and protect applications at runtime specially from Zero Day Attacks.	The Solution should protect applications at runtime specially from Zero Day Attacks
35	74	WAF	Server Load Balancing for non-http application also then include the following point	Clause deleted
36	76	Web Proxy with DLP	Also the solution must have the option to allow or deny a particular domain or destination for a user or IP group for a permanently or for a specific time period. Solution should be able to block domains which are containing alpha numeric and special characters.	The solution must have the option to allow particular domain or destination for a user or IP group for a permanently or for a specific time period. Solution should be able to block domains which are containing alpha numeric and special characters.
37	79	Web Proxy with DLP	Solution should be able to restrict Users to download certain files based on file types, size, extensions etc. Also the solution should be capable of blocking specific set of files downloads for specific user groups. Even if the file types are blocked globally,exception based on URLs, IPs, domains should be allowed.	Solution should be able to restrict Users to download certain files based on file types, extensions etc. Also the solution should be capable of blocking specific set of files downloads for specific user groups. Even if the file types are blocked globally, exception based on URLs, IPs, domains should be allowed.
38	81	Web Proxy with DLP	solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read- only access user.	Solution shall support role-based administration such as Administrator, Database Reader, and Read- only access user.
39	81	Web Proxy with DLP	solution should support a web interface that includes a tool that traces & can simulate client requests as if they were made by the end users. It should describe how Web Proxy processes the request and can be used for troubleshooting purpose. It should also support policy simulating functionality.	Solution should support a web interface that includes a tool that traces user activities and provide test policies to test the environment before applying to users.
40	83	Web Proxy with DLP	The centralized management should be provided without the support of additional hardware/server (preferably) and if any additional devices required for the management of solution, it should be mentioned clearly.	The centralized management solution should be provided and additional hardware/server if required for the management of centralized management solution, it should be mentioned clearly.

41	86	General	The Solution should be capable of retrieving the logs for analysis, reporting, and forensic purposes.	Clause deleted
42	86	CLMS	The Solution should be licensed based on the EPS count (and not licensed by the number of users, device types, and/or the number of network or end systems devices that are subject to logging).	The Solution should be licensed for 5000 EPS or 1000 devices (and not licensed by the number of users, device types, that are subject to logging).Please refer to modified commercial bid
43	90	DAM	The solution should provide optimum utilization of resources by using Load balancing between its devices, if it is using multiple boxes/gateways The solution should send all audit logs to centralised log management server.	“The solution should provide optimum utilization of resources on the database monitoring. The solution should send all audit logs to centralised log management server.”
44	108	Patch Management	The solution should support local distribution points through preferred servers and endpoints and also peer downloading	The solution should support local distribution points through preferred servers and endpoints
45	108	Patch Management	The Agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.	The solution should have a fall back mechanism where the agent should connect with Central server if the assisgned distribution server is not available
46	112	Asset and Patch Management	The solution should support PCI compliance/ OVAL/ SCAP scan for integrated endpoints.	Clause deleted
47	114	VAS	The proposed solution should provide mechanism to upload IP lists of devices through XLS format	The proposed solution should provide mechanism to upload IP lists of devices through XLS format/Text Format
48	116	SIEM	Security Incident and Event Management (SIEM) - 5000 EPS New Licenses, 1000 Device Licenses	Security Incident and Event Management (SIEM) - 5000 EPS New Licenses
49	119	Blacklisting Clause	We hereby undertake and agree to abide by all the terms and conditions including all Annexure, Corrigendum(s) etc. stipulated by the Bank in this RFP. Any deviation may result in disqualification of our bid. We understand & agree that in event of being successful in the bid, we shall comply to the terms & conditions of RFP in future and shall not attempt to get the same changed from Bank later on in process of implementation, contract signing, and extension of contract and / or subsequent purchase order/s from Bank. We understand and agree that such attempts and non-compliance to RFP terms may lead to cancellation of	We hereby undertake and agree to abide by all the terms and conditions including all Annexure, Corrigendum(s) etc. stipulated by the Bank in this RFP. Any deviation may result in disqualification of our bid. We understand & agree that in event of being successful in the bid, we shall comply to the terms & conditions of RFP in future and shall not attempt to get the same changed from Bank later on in process of implementation, contract signing, and extension of contract and / or subsequent purchase order/s from Bank. We understand and agree that such attempts and non-compliance to RFP terms may lead to cancellation of our

			our Contract and suitable penal action may be taken by Bank against us including invoking the EMD and/ or PBG and blacklisting.	Contract and suitable penal action may be taken by Bank against us including invoking the EMD and/ or PBG.
50	145	Checklist	THE BIDDER MUST HAVE THEIR CAPTIVE SOC FOR LAST 5 YEARS IN INDIA PROVIDING SECURITY SERVICES TO VARIOUS PUBLIC/PRIVATE COMPANIES/ORGANISATIONS	THE BIDDER MUST HAVE THEIR CAPTIVE SOC IN INDIA PROVIDING SECURITY SERVICES TO VARIOUS PUBLIC/PRIVATE COMPANIES/ORGANISATIONS
51		All Possible solutions	Additional Clause-Specifications	1. Any centralized console required as part of EDR, asset management, patch management, SIEM and PIM can be configured as individual instances for each bank for better manageability. 2. Wherever possible in the hardware level, there should be at least virtual partitions to isolate the three bank's configuration, traffic at the most possible way to avoid any dependencies for any day to day operations.

SECTION 5 - COMMERCIAL BID

(on Bidder's letterhead)

[SETTING UP OF CYBER SECURITY OPERATION CENTER (CSOC) IN TNGB,SGB AND PBGB]

TABLE -A

PROCUREMENT OF DEVICES/ SOLUTIONS WITH 3 YEARS WARRANTY and its AMC
(All amount should be in INR inclusive all taxes)

S.No.	Item Description	Make and Model/ Part Number	Multiplication Factor	Procurement Cost with 3 years warranty		AMC Cost for 4th and 5th Year			Total Cost
			[A]	Unit Cost [B]	Total Cost [C]=[A*B]	AMC cost for 4th Year [D]	AMC cost for 5th Year [E]	Total AMC Cost [F] = D+E	[G] = [C] + [F]
1	Internal firewall		04						
2	External firewall		04						
3	WAF		**04**						
4	NTP		02						
5	VAS		01						
TOTAL OF TABLE -A									

TABLE -B

PROCUREMENT OF SOLUTIONS WITH LICENSES [WITH 1-YEAR WARRANTY AND 4 YEARS ATS OR SUBSCRIPTION LICENSE] (All amount should be in INR inclusive all taxes)

S.No.	Item Description	Make and Model/ Part Number	Multiplication Factor	Procurement Cost with 1 years warranty		ATS Cost for 2nd, 3rd, 4th, 5th Year					Total Cost [F] = [C] + [E]
			[A]	Unit Cost [B]	Total Cost [C]= [A*B]	2nd Yr AMC [D]	3rd Yr AMC [E]	4th Yr AMC [F]	5th Yr AMC [G]	Total AMC Cost [H] = [D+E+F+G]	Total Cost [I] = [C +H]
6	Database Activity Monitoring (DAM) Solution		10 DB Licenses								
7	Asset Management and Patch Management		6500 device licenses for patch management and 5500 device licenses for asset management								
8	Centralised Log Management Solution (CLMS)		200 Licenses								

9	Web Proxy Solution with Web DLP		3500 new users								
10	Security Incident and Event Management (SIEM)		5000 EPS New Licenses								
11	Privilege Identity Management [PIM]	Arcos	50 Existing Licenses, Renewal of ATS till end of contract period								
12	Endpoint Detection Response		5500 licenses								
TOTAL OF TABLE - B											

TABLE- C:

FACILITY MANAGEMENT SERVICES [ONSITE TECHNICAL SUPPORT] FOR A PERIOD OF FIVE (5) YEARS

*All amount in INR

S.No.	Item Description	Unit Cost per Year [A]	No. of Resources [B]	No of Years [C]	Total cost [D] = [A*B*C]
1	L2 Resource		3	5	
2	L1 Resource			5	
TOTAL OF TABLE - C					

* - All amount should be quoted in INR inclusive of all taxes.

TABLE- D:

ONE TIME IMPLEMENTATION COST

*All amount in INR

S.No.	Solution Description	Quantity (Considering both DC and DRS) [A]	Unit Implementation Cost [B]	Total Implementation Cost [C] = [A*B]
1				
2				
3				
4				
			TOTAL OF TABLE - D	

* - All amount should be quoted in INR inclusive of all taxes.

TABLE- E:			
TOTAL COST OF OWNERSHIP (TCO) FOR FIVE YEARS PERIOD			
			*All amount in INR
S.No.	**Table Detail**	**Table Description**	**Total Cost**
1	Total of Table A	Procurement of Devices/ Solutions With 3 Years Warranty with AMC	
2	Total of Table B	Procurement of Solutions with Licenses [with 1-Year Warranty and 4 Years ATS/AMC/Subscription]	
3	Total of Table C	Facility Management Services [Onsite Technical Support] for a period of five (5) years	
4	Total of Table D	One Time Implementation Cost	
		TOTAL OF TABLE - E	

* - All amount should be quoted in INR inclusive of all taxes.

தமிழ்நாடு கிராம வங்கி
TAMIL NADU GRAMA BANK
(A Government owned Bank Sponsored by Indian Bank)

Clarifications to the RFP No: TMD/10/2023-24 dated 04/09/2023

Sl No	Page No	Type	Clause No	RFP Clause	Bidder Clarification	Response/Clarification
1	3	Bid Timelines	General Tender Details	Last date and time for Online bid submission (both Technical & Commercial) 27/09/2023, 15:00 Hrs	Request you to please extend the proposal submission date by another two weeks i.e. **11/10/2023 up to 15.00 hours.**	Please refer to the GeM portal for bid submission timelines
2	7	SCOPE OF WORK.	5	Bidder to provide new solution for 5500 EDR on an annual subscription basis. Bank will provide system requirement in VM environment at DC and DRS for the solutions. The solution should be scalable for future expansion and needs.	In the Scope of work section of the RFP, deployement of EDR solution is mentioned. To reduce the operational overhead it is very improtant to minimiz the number of dashboards. We recommend TNGB to have an EDR solution integrated with SIEM platform. We would also like to request TNGB to please include below mentioned features to get the maximum benifits out of the EDR solution. 1. EDR solution should support all flavors of Linux, Windows, UNIX and Mac OS. 2. The solution must support the means to execute and assist with forensic investigation. 3. Solution should have capability to obtain memory dump. 4. The solution must provide encrypted communication between the central EDR server and the agents on the endpoints or servers. Solution should support centralized agent upgrade, directly from UI. 5. Solution should automatically initiate a quick, targeted scan when unknown files, processes and more load on an endpoint, record data about every critical action (e.g., file or registry modifications, network connections) surrounding the unknown item, and communicate to the management server Solution should support analysis of advanced attacks such as system exploitation, data exfiltration, etc. 6. Solution should provide Anomaly detection like, Image Hooks, Kernel Hooks, Registry Discrepancies, Suspicious Threads, etc. 7. Solution should have capability to block files with the following file extensions like, but not limited to EXE, COM, SYS, DLL, BAT, PS1, VBS, VBE, VB, etc.	Please adhere to the terms and conditions of the RFP

3	7	1. SCOPE OF WORK. Security Incident and Event Management (SIEM)	8	Bank intends to procure SIEM solution for DC and DRS with 5000 EPS. The solution should be scalable for future expansion and needs.	In the Scope of work section of the RFP, deployement of SIEM solution is mentioned. The detailed scope of work or the specifications are not mentioned. Looking at the criticality of the project and the amount of critical data it will be handling (5,000 EPS), the detailed specification or the use cases should be mentioned clearly. This will not only help TNGB to get a proper solution as per their requirement but also help in validating the capability of the product. We would also like to request TNGB to please include below mentioned features to get the maximum benifits out of the SIEM solution. 1. SIEM solution should provide the collection of events through customization of connectors or similar integration. Must support event collection using at least the following industry standards: Syslog, ODBC, SNMP, SDEE, VMware, File, Checkpoint Lea, AWS, Windows. etc. should not have any limit on the number of collectors 2. Next generation platform shall encompass log data with added context and threat intelligence. It should have single console for Packet/Deep Packet inspection and EDR solution to provide complete network and endpoint visibility through deep packet inspection, high speed packet capture and analysis. 3. The system shall allow automated functionality for the archival of data based on data retention policy. Data retention policy must be configurable on various parameters but not limiting to compliance requirements, device type, available storage, event type etc. 4. The Analyst UI must be a common interface to investigate data collected and normalized for SIEM (Logs) and DPI (Packet data) with logs and packet correlation using same rule. 5. The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs, endpoint, and packets. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle. 6. The Solution should have a monitoring interface for resource utilization like CPU, memory for different SIEM components like collector, aggregator, Correlation engine, etc. 7. The proposed solution should provide the ability to transmit alerts using multiple protocols and mechanisms to other solutions such as SMTP, syslog etc. 8. The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like Firewall, IPS, HIPS, AV, DLP, and Encryption. This will ensure defense in depth strategy so that threats missed by existing	Please adhere to the terms and conditions of the RFP

					technologies can be detected at SIEM level. 9. All logs should be automatically categorized into categories like Firewall, IPS, Operating System, etc. Every information in the logs should be normalized to a common format across devices.	

4	7	1. SCOPE OF WORK. Security Incident and Event Management(SIEM)	8	Bank intends to procure SIEM solution for DC andDRS with 5000 EPS. The solution should be scalablefor future expansion and needs.	We would like to request TNGB team to include below mentioned points to enhance the functionality of SIEM platform in terms of Deep Packet Inspection to gain complete visibility.1. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data should .2. Solution should store raw packet data for 7 days and normalized packet data for 15 days for forensics.3. The solution should support full session reconstruction and object extractions from sessions like files and pcaps.4. The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure.5. Solution should have unified console for threat detection using Logs, Packet Capture for compete correlation on all aspects.6. Solution should create indexes for payload objects and not just rely on header information to augument investigation capabilities	Please adhere to the terms and conditions of the RFP
5	8	Service conditions	2	Bank also intend to identify a Security Services Vendor for supplying, installation, upgradation, configuration, commissioning, maintenance and Facility Management Services for existing as well as new security solutions, for a period of Five (5) years through this Open Tendering Procurement Process through GeM (Government e-Marketplace) portal.	Kindly clarify if the contract duration of 5 years is post implementation / Go Live / Sign off or inclusive of it. Our suggestion is to have it as 5 years operations and maintenance phase post implementation / Go Live / Sign off.	It is clarified that contract date commences from date of sign off for appliance based solutions and for other solutions, it is from date of delivery.
6	8	Contract Entity	1. Introduction Contracting Entity	1. Introduction Contracting Entity	Requesting the Bank to kindly clarify what entities will be the Contracting Entity with the Bidder - TNGB (or) all 3 entities.	It is clarified that all three RRBs will be contracting entities. However TNGB will be front ending the project.
7	8	Payment Terms	Payment Terms	NA	Please confirm whether payment will be made within 30 days of receipt of invoice	Accepted

8	9	PRE-QUALIFICATION CRITERIA OF THE BIDDER	3	a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.	A) We would request a bank to modify this clause - The bidder should have supplied, deployed, and managed CSOC setup comprising SIEM, WAF, and EDR Solutions from the last 3 years in at least one Government, private or public Banking and Financial Institution/organization in India. d) We request the bank to modify this clause - All solutions mentioned above (SIEM, WAF, and EDR) should be from any OEM and bidders should have experience with the technology proposed for this tender.	Please refer to the amendment
9	9	PRE-QUALIFICATION CRITERIA OF THE BIDDER	3	3. Pre-qualification criteria of the Bidder Eligibility Criteria, Point 3: a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India.	Requesting the Bank to change this clause as: "a) The bidder should be managing CSOC setup comprising SIEM, WAF and EDR Solution, and operational as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India."	Please refer to the amendment
10	9	PRE-QUALIFICATION CRITERIA OF THE BIDDER	3	3. Pre-qualification criteria of the Bidder Eligibility Criteria, Point 3: d) All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender	Requesting the Bank to consider technology implementations in similar organizations rather than specific make. Kindly amend this clause as: "d) All solutions mentioned above (SIEM, WAF and EDR) can be of any make for this tender."	Please refer to the amendment

11	9	PRE-QUALIFICATION CRITERIA OF THE BIDDER	3	3 a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.	Kindly requesting for clarification for the criteria under the Sl No. 3,Point d : "All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender." > Point (d) is categorized under the OEM Criteria within the Bidder Qualification criteria, and it appears to provide an advantage to a specific OEM, potentially discouraging the participation of other innovative and highly capable OEMs. We kindly request the consideration of exempting this clause in order to promote a more inclusive opportunity for a broader range of qualified OEMs.	Please refer to the amendment
12	9	Pre Qualification Criteria	3.3	3 a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b)Any two of the above three solutions should be supplied by the bidder and running in a single company.c)The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders.d)All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.	Kindly requesting for clarification for the criteria under the Sl No. 3, Point d : "All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender." > Point (d) is categorized under the OEM Criteria within the Bidder Qualification criteria, and it appears to provide an advantage to a specific OEM, potentially discouraging the participation of other innovative and highly capable OEMs. We kindly request the consideration of exempting this clause in order to promote a more inclusive opportunity for a broader range of qualified OEMs.	Please refer to the amendment
13	9	Pre Qualification Criteria	3.3	a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) All solutions mentioned above (SIEM, WAF	Request to Remove this clause - d)All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender	Please refer to the amendment

				and EDR) should be of same make proposed for this tender.		
14	9	Pre-qualification Financials	3. Pre-qualification criteria of the Bidde	3. Pre-qualification criteria of the Bidder Eligibility Criteria, Point 4: The Bidder should have minimum average turnover of Rs.80 Cr. (Rupees Eighty Crores only) in each of the last 3 financial years. Bidder must provide the details of turnover for last 3 years (FY-2020-21, 2021-22, 2022-23)	The financials for FY22-23 are currently under audit and not available to share with the Bank. We can share the financials for FY19-20, FY20-21, and FY21-22. Please confirm.	It is clarified that unaudited balance sheet signed by company auditor for the years for which audited balance sheet is not available is accepted.
15	9	Pre-qualification balance sheets and P&L	3. Pre-qualification criteria of the Bidde	3. Pre-qualification criteria of the Bidder Eligibility Criteria, Point 5: The Bidder should have positive net worth and should not have been eroded by more than 30% during the last three consecutive financialo years (Balance sheet and Profit & Loss statement certified by CA) have to be submitted.	We can share the CA certified balances sheets and Profit & loss statements for the years FY19-20, FY20-21, and FY21-22, as financials for FY22-23 are currently under audit and not available to share. Please confirm.	It is clarified that unaudited balance sheet signed by company auditor for the years for which audited balance sheet is not available is accepted.
16	9	Pre-qualification CSOC Setup	3. PRE-QUALIFICATION CRITERIA OF THE BIDDER Sr. No-3	a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF and EDR Solution on or before 31/03/2020 and continue to run as on 31/03/2023 in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.	Kindly amend the clause as: a) The bidder should have supplied, deployed and managing CSOC setup comprising SIEM, WAF/NGFW and EDR Solution on or ~~before~~ after 31/03/2020 and continue to run for minimum 1year as on ~~31/03/2023~~ bid submission date in at least one Government, private or public Banking & Financial Institutions/organizations in India. b) Any two of the above three solutions should be supplied by the bidder and running in a single company. c) The solutions meeting criteria 3-b (two solutions running in a single company) may have different purchase orders. d) ~~All solutions mentioned above (SIEM, WAF and EDR) should be of same make proposed for this tender.~~	For Clause 3-a, please refer to the amendment. For Clause 3-d, It is clarified that the bidder is expected to have experience by implementing the make of solution proposed for this tender for other clients of the bidder. However it is not required that SIEM, WAF and EDR must be of same OEM.
17	9	Liquidated Damages	Liquidated Damages	NA	Please confirm whether there are any LDs for SLA breaches over and above the penalties	It is clarified that LDs are related to delay in deliveries and SLAs are related to services

18	9	SIEM	Microfocus - SIEM	The proposed solution should be sized for 5,000 sustained EPS at correlation layer initially per Data centre but should be able to handle peak >License deployed EPS (additional 5000 EPS to take care of spikes/ burst / outbreak / flood in traffic) at correlation layer without dropping events or queuing events (for SIEM) per Data Centre.	Please confirm on the total data centers in scope for SIEM to size the comlpete solution, going by the propotion of 5000 EPS per data center	The requirement is expected for two Data centers
19	9	Bidder turnover	Pre-Qualification Criteria of The Bidder	Bidder should have minimum average turnover of Rs.80 Cr. (Rupees Eighty Crores only) in each of the last 3 financial years. Bidder must provide the details of turnover for last 3 years (FY-2020-21, 2021-22, 2022-23).	**Request to modify the clause as below:** Bidder should have minimum average turnover of Rs.**50 Cr.** in last 3 financial years. Bidder must provide the details of turnover for last 3 years **(FY-2020-21, 2021-22 as per the last published audited balance sheets AND FY 2022-23 (as per Provisional Certificate)**	Please adhere to terms and conditions
20	10	Pre Qualification Criteria	3.9	The bidder should have captive SOC in their premises live from or before 31 Mar 2020 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.	Request to Amend the clause-The bidder should have captive SOC in their premises live from or before 31 Mar 2023 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023	Please adhere to the terms and conditions of the RFP
21	10	PRE-QUALIFICATION CRITERIA OF THE BIDDER	9	The bidder should have captive SOC in their premises live from or before 31 Mar 2020 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.	Request bank to modify this clause - The bidder should have captive SOC in their premises live from the last 3 years providing remote services from their SOC to a minimum one client with 5000 EPS.	Please adhere to the terms and conditions of RFP.
22	10	Pre-qualification CSOC Setup	9	The bidder should have captive SOC in their premises live from or before 31 Mar 2020 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.	This clause is restrictive and biased in nature. Request to modify the clause as **The bidder should have captive SOC in their premises and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023**	Please adhere to the terms and conditions of RFP
23	10	Pre-qualification CSOC Setup	10	The bidder should be providing SOC services in customer premises with SIEM of 5000 EPS for minimum two customers on or before 31/03/2020 and should continue to provide the service to the customers as on 31/03/2023.	This clause is restrictive and biased in nature. Request to modify the clause as **The bidder should be providing SOC services with SIEM of 5000 EPS for minimum two customers as on 31/03/2023.**	Please adhere to the terms and conditions of RFP
24	10	OEM eligibility	PRE-QUALIFICATION CRITERIA OF THE BIDDER	The offered solution's OEM should have Technical support centre in India.	Requesting Bank to amend " All the OEMs should have support team based out of India".	Please adhere to the terms and conditions

25	10	SIEM	3. PRE-QUALIFICATION CRITERIA OF THE BIDDER Sr. No-10	The bidder should be providing SOC services in customer premises with SIEM of 5000 EPS for minimum two customers on or before 31/03/2020 and should continue to provide the service to the customers as on 31/03/2023	Kindly amend the clause as: The bidder should be providing SOC/Cyber security services in customer premises with SIEM ~~of 5000 EPS~~ for minimum two customers on or after ~~before~~ 31/03/2020 and should continue to provide the service to the customers as on 31/03/2023	Please adhere to the terms and conditions of RFP
26	10	Pre-qualification CSOC Setup	3. PRE-QUALIFICATION CRITERIA OF THE BIDDER Sr. No-9	The bidder should have captive SOC in their premises live from or before 31 Mar 2020 and providing remote services from their SOC to minimum one client with 5000 EPS as on 31/03/2023.	Kindly amend the clause as: The bidder should have captive SOC in their premises live from ~~or before~~ 31 Mar 2022 and providing remote services from their SOC to minimum one client ~~with 5000 EPS~~ as on 31/03/2023.	Please adhere to the terms and conditions of RFP
27	10	Inspection	4. Right to Audit	Bank shall have the right to conduct audits on the service provider by its internal or external auditors, or by agents appointed to act on its behalf and to obtain any copies of any review reports and findings made on the service provider in conjunction with the services performed for the bank. The bidder should allow RBI/NABARD or persons authorized by RBI/NABARD to access the Bank’s documents, records of transactions and other necessary information given to, stored or processed by the service provider / Sub-Service provider within a reasonable time. This includes information maintained in papers and electronic formats. The Service provider shall recognize the right of the regulatory authorities to cause an inspection to be made of their books and account by one or more of its officers or employees or other persons.	We propose to modify as follows:- At TNGB ’s sole cost and expense, TNGB or its accredited auditor may audit Tata Communication’s ("TC")Facilities and related records and documents solely pertaining to TC ’s provisioning of Services to Customer during the Service Term of the audited Service. TNGB shall provide TC not less than thirty (30) days’ prior written notice of any such audit request provided, however, if TNGB ’s audit request is directly related to compliance with any directives of a Governmental Authority and TNGB provides reasonably acceptable documentation of such request, TC will endeavour to meet such other timelines as may be reasonably required by such Governmental Authority. Subject to the Auditor entering into a confidentiality agreement with TC on reasonably acceptable terms, the Parties shall each, at their own cost, reasonably co-operate with the Auditor and provide reasonable non-privileged information requested by the Auditor relating to the audited Services, (including making available knowledgeable personnel and pertinent documents and records, e.g., copies of ISO, ISAE or other relevant reports or certifications) to assist in formulating and appropriately limiting the scope of the audit. The scope and proposed audit schedule shall be mutually agreed by the Parties. TNGB will perform such audit during TC's normal business hours, not more than one (1) time in any calendar year during the Service Term of the audited Service in accordance to generally accepted auditing standards. Any audit conducted by or on behalf of TNGB shall be conducted with the utmost integrity, employing an acceptable level of skill and technical knowledge.	It is clarified that TNGB will provide advance written notice to the successful bidder for commencing the audit if audit is required. The cost for the audit will be borne by the bank.

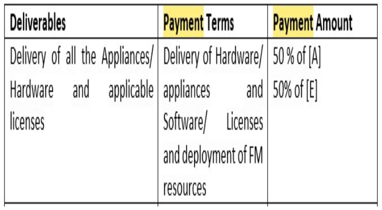
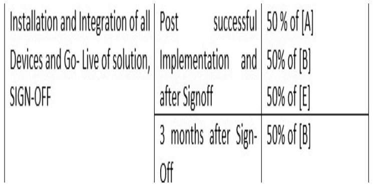
28	10	Joint Bid clause	5. OTHER CONDITIONS	b) Joint bid will not be accepted by the Bank.	Request to allow **Joint Venture/ Consortium/ Subcontracting (1 Lead member + 1 Consortium Member)** **Reason:** We are a Managed Security Service Proivder having all the required expertise and resources to manage SOC operations. The tender has a requirement to provide the on-prim set-up of SOC services for which we have extensive prior experience. **However, the qualification and experience asked w.r.t. on-prim set-up restricts us from participating in the bid.** We are keen to participate in the bid in a "joint consortium", providing a mix of expertise in the areas of SOC services as well as procurement and installation services respectively by both parties of the consortium. Hence, it is **requested to allow consortium/Joint bid for the tender.**	Please adhere to the terms and conditions
29	10	CLMS	OEM - CLMS Queries	11.The offered solution's OEM should have Technical support centre in India	Request you to please remove this clause as the support is remote and over phone	Please adhere to the terms and conditions
30	10	OEM eligibility	OEM eligibility	The OEMs who have provided network devices for bank's network (LAN and WAN) are not eligible to participate in this CSOC project RFP as the bank should have different OEMs for network and CSOC as per industry best practices.	Requesting the Bank to name the current OEMs taking care of the Bank's network (LAN and WAN) so that we can ensure to bring other OEMs onboard for this project.	SIs may contact OEMs to know their eligibility
31	11	Man Power	5 (f)	a) Each L2 resource should have certification in 2 or more solutions.	We request the bank to relax it to 1 certification per L2 resource. We also request the bank to specify the certification details expected by the bank.	Please adhere to the terms and conditions of RFP
32	11	Man Power	5. Other Conditions Point f: Each L2 resource should have certification in 2 or more solutions	5. Other Conditions Point f: Each L2 resource should have certification in 2 or more solutions	Requesting the Bank to change this clause as: "Each L2 resource should have certification in 1 or more solutions"	Please refer to the amendment
33	11	Man Power	5. OTHER CONDITIONS Sr.No g)	All the resources deployed by the bidder should be in the payroll of the successful bidder	Request to allow subcontracting of L1 Resources.	No change. Please adhere to the terms and conditions of the RFP

34	11	Man Power	5. OTHER CONDITIONS Sr.No g)	All the resources deployed by the bidder should be in the payroll of the successful bidder	Payroll of the bidder shall mean proof of deduction of PF for the staff deployed by the bidder, please confirm	It is clarified that following indicative list of documents should be produced whenever requested by the bank 1- PF/NPS Statement, 2 - Pay slip from employer 3 - Identity card, 4 - Form 16 from employer
35	11	WAF	A10 - WAF	The WAF solution should not be any white labelled or 3rd party WAF solutiondeployed on any OEM hardware/software.	The white labelled WAF offer the best of the breed WAF solution included with a reverse proxy-ADC.We are present in Gartners Magic quadrant since last 3 years and also the latest Gartners WAAP 2022 magic quadrant. It offers strong application security viz. OWASP top 10, API, MicroServices, ATO etc. Request you to remove this caluse as this will restric such OEM to bid.	Please adhere to the terms and conditions of RFP
36	11	WAF	WAF	The WAF solution should not be any white labelled or 3rd party WAF solution deployed on any OEM hardware/software.	The white labelled WAF offer the best of the breed WAF solution included with a reverse proxy-ADC.We are present in Gartners Magic quadrant since last 3 years and also the latest Gartners WAAP 2022 magic quadrant. It offers strong application security viz. OWASP top 10, API, MicroServices, ATO etc. Request you to remove this caluse as this will restric such OEM to bid.	Please adhere to the terms and conditions of RFP
37	12	DAM	Imperva DAM	The solution should audit all types of database access across the organization regardless of database type or operating system of the host without relying on native auditing.	For OS not supported by agents, native audtining may be required for monitoring	Please adhere to the specifications
38	14	Bid Validity	5. VALIDITY OF BID DOCUMENT	Bid shall remain valid for 6 months from last date of submission of bid prescribed by Bank	Majority of the OEMs offers a product validity of sixty to ninety days. Hence request to amend the clause as follows: "*Bid shall remain valid for ~~6~~* ***3*** *months from last date of submission of bid prescribed by Bank*"	Please refer to the terms and conditions of the RFP

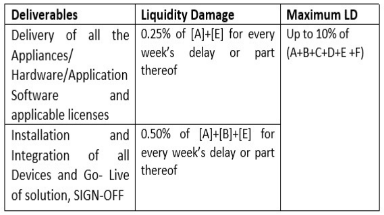
39	14	Bid Earnest Money	7. Bid Earnest Money	Bidder has to submit the Earnest Money Deposit (EMD) of Rs.40 Lakhs (Rupees Forty Lakhs Only) (Registered MSE and Start-up India bidder is exempted from payment of Earnest Money Deposit if bidder can furnish requisite proof subject to the satisfaction of Bank), which should be submitted in the form of Bank Guarantee (BG) favouring Tamil Nadu Grama Bank, TMD Department, Salem. The BG should have a validity of 9 months from the date of submission of bid with claim period of 12 months. The BG should be submitted at the time of Bid submission. Start-up bidder recognized by Department of Industrial Policy and Promotion (DIPP) is also exempted from payment of Earnest Money Deposit.	As per the General Terms and Conditions on GeM 4.0 (Version 1.12) dt 16th August 2023, The Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s) are exempted from furnishing the Bid Security. Kindly confirm on this.	Accepted
40	15	Bid Submission	8. BIDDING PROCESS	Bidders are required to strictly submit their bids in electronic form on GeM Portal followed by Submission of Hardcopy of Earnest Money Deposit (EMD) and Integrity pact documentations, on address as mentioned above. The Commercial Bids has to be submitted in only online form through GeM Portal	We understand both Technical & Commercial bid needs to be submitted online and only EMD and Integrity Pact original Hardcopy needs to be submitted post online submission. Kindly confirm	It is clarified that the understanding is correct
41	17	QCBS	14. Evaluation and Award Criteria:	14. Evaluation and Award Criteria: i) Evaluation of Bids:	Considering the complexity of this RFP involving multiple security technologies, requesting the Bank to consider Quality cum Cost-Based Selection (QCBS) as the evaluation and award criteria, and select the successful bidder based on T1-L1 scoring.	Please adhere to the terms and conditions of RFP

42	18	Force Majeure	17	Force Majeure	1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure.2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor’s fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days.3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the bidder shall hold consultations in an endeavour to find a solution to the problem.5) Notwithstanding above, the decision of Tenderer shall be final and binding on the bidder regarding termination of contract or otherwise	Please adhere to the terms and conditions of RFP.
43	18	MII	Procurement through local successful bidder/vendors	Make in India: The bidder will have to submit a self certification that the offer items meets the minimum local content and shall given details of the locations at which the local value addition is made.	Since most of the cyber security appliances, licenses, hardwares are from the globally renowned OEMs. Meeting Make In India guidelines is very tough. Hence request to keep the make in India guidelines for selection of bidders as optional need not be mandatory.	Please refer to the terms and conditions of the RFP
44	18	CLMS	Section 15	Preference to Make in India	Request you to please relax the preference to Make in India, so that non make in India products get the same weightage as the make in India products.	Please adhere to the terms and conditions of RFP
45	18	MII	Section 15	Make in India clause :	Request you to remove or Can we remove this clause ?	Please adhere to the terms and conditions of RFP

46	19	Performance Bank Guarantee	21. PERFORMANCE BANK GUARANTEE Sr. No. a)	The successful bidder will have to submit Performance Bank Guarantee amounting to 10% of Contract value within one month from purchase order issued & initially valid for a period of 5 years from the date of contract with claim period of another additional 12 months.	As per the Notification No. F.9/4/2020-PPD from the Ministry of Finance, in all the govt. Projects PBG has been recommended to 3% of contract value. Hence, we request to amend the clause as: " *The successful bidder will have to submit Performance Bank Guarantee amounting to ~~10%~~ **3%** of Contract value within one month from purchase order issued & initially valid for a period of 5 years from the date of contract with claim period of another additional 12 months*."	It is clarified that as per Notification No. F.9/4/2020-PPD, the validity is till 31-03-2023 only. Please adhere to the terms and conditions of the RFP
47	20	Man Power	24	All the delivered Product/Solution/Software items may be subjected to an acceptance test. Successful bidder has to arrange onsite support personnel at the date and time mentioned by the Bank to assist in the acceptance test.	We request the bank to kindly confirm if operations start date is one month post implementation or 90 days from the date of PO whichever is earlier or only after the acceptance test is being approved by the bank.	It is clarified that operations start date is one month post implementation or 90 days from the date of PO whichever is earlier
48	20	Payment Terms	25	Payment terms : Hardware, Software, Licenses and FMS	Request to change payment terms as 80% on delviery and 20% post license activation; FMS - Quarterly in advance;AMC/ATS charges to be paid yearly in advance	Please refer to the amendment
49	20	GST	25. PAYMENT TERMS	Only GST, wherever applicable, will be borne by the Bank	Please confirm that any change in statutory Taxes and Duties including introduction of new levies if any shall be borne by Department at actuals against submission of documentary proof.	It is clarified that Only GST, wherever applicable, will be borne by the Bank.
50	20	Payment Terms	25.Payment Terms	Delivery of all the Appliances/ Hardware and applicable licenses On submission of Performance Bank Guarantee (PBG), Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources 50 % of [A]-Device Cost 50% of [E]-License Cost	**OEM's collects 100% aginest delivery from SI's, the current payment term seriously impact the Cash Flow** , Hence requesting the Bank to modify the caluse as " Delivery of all the Appliances/ Hardware and applicable licenses On submission of Performance Bank Guarantee (PBG), Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources 70 % of [A]-Device Cost 70% of [E]-License Cost	Please refer to the amendment
51	20	Payment Terms	25.Payment Terms	Requesting Bank to modify the caluse as " Installation and Integration ofall Devices and Go-Live of solution, SIGN-OFFPost successful Implementation and after Signoff50 % of [A] -Device Cost50% of [B]- Implementation Cost50% of [E] -License Cost 3 months after Sign- Off 50% of [B] - Implementation Cost	Requesting Bank to modify the caluse as " Installation and Integration ofall Devices and Go-Live of solution, SIGN-OFFPost successful Implementation and after Signoff30 % of [A] -Device Cost70% of [B]- Implementation Cost30% of [E] -License Cost 1 months after Sign- Off 30% of [B] - Implementation Cost	Please refer to the amendment

52	20	Payment Terms	25.Payment Terms	AMC/ ATS cost of Devices/ Solutions/ Components Shall be paid half yearly in advance on submission of Invoices and requisite documents. This will start post expiry of warranty as applicable	**OEM's collects 100% yearly advance from SI's, the current payment term seriously impact the Cash Flow** Hence requesting Bank to modify the caluse as " AMC/ ATS cost of Devices/ Solutions/ Components Shall be paid 100% yearly in advance on submission of Invoices and requisite documents. This will start post expiry of warranty as applicable"	Please adhere to the terms and conditions of RFP
53	21	Man Power	25	Facility management services (F) - Shall be paid quarterly in arrears on submission of Invoices and requisite documents	We request the bank to consider quarterly in advance payment for the FMS services	Please adhere to the terms and conditions of RFP
54	21	Invoices	25	For endpoints bases licenses like EDR, Asset management, Patch management etc., the invoices shall be raised to three Regional Rural Banks separately for which the break up licenses will be informed to successful bidder.	We request the bank to kindly amend this clause and allow the bidder to raise invoice to TNGB only. We also request TNGB to take complete ownership for all the payments.	Please adhere to the terms and conditions. However TNGB will take complete ownership for all the payments due.
55	21	25. Payment terms	25	 **Deliverables** | **Payment Terms** | **Payment Amount** Delivery of all the Appliances/ Hardware and applicable licenses | Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources | 50 % of [A] 50% of [E]	Request to Change 50% of A to 75% of A and 50% of E to 75% of E	Please refer to the amendment.
56	21	25. Payment terms	25	 Installation and Integration of all Devices and Go- Live of solution, SIGN-OFF | Post successful Implementation and after Signoff | 50 % of [A] 50% of [B] 50% of [E] | 3 months after Sign-Off | 50% of [B]	Request to Change 50% of A to 25% of A ,Change 50% of B to 75% of B 50% of E to 25% of E	Please refer to the amendment.
57	21	Invoices	25 (Payment Terms)	For endpoints bases licenses like EDR, Asset management, Patch management etc., the invoices shall be raised to three Regional Rural Banks separately for which the break up licenses will be informed to successful bidder.	If the bank is expecting the breakup of licenses, does it mean that there will be multiple different management consoles for these regional bank or it is just for the purpose of invoicing only, please clarify.	It is clarified that the breakup of licenses meant the different management console for each Bank and invoicing should be charges as per the licenses.

58	21	Payment Terms	25. PAYMENT TERMS	a)Delivery of Hardware/ appliances and Software/ Licenses and deployment of FM resources - 50 % of [A] & 50 % of [E] b)Post successful Implementation and after Signoff 50 % of [A] , 50% of [B] & 50% of [E] c)3 months after SignOff : 50% of [B]	The current payment terms is affecting the bidder's cash flow. Hence request to consider the below payment terms: "a) Delivery of Hardware/ appliances and Software/ Licenses ~~and deployment of FM resources~~ - 70 % of [A] & 80 % of [E] on prorata basis b)Implementation of Hardware/ appliances and Software/Licenses 20 % of [A] , 90% of [B] & 10% of [E] on porata basis *c)*Go- Live of solution, SIGN-OFF 10 % of [A] , 10% of [B] & 10% of [E] "	Please refer to the amendment
59	21	Billing of man power resources	25. Payment Terms:	25. Payment Terms: - For endpoints bases licenses like EDR, Asset management, Patch management etc., the invoices shall be raised to three Regional Rural Banks separately for which the break up licenses will be informed to successful bidder. - For centralized solutions like Firewall, WAF etc, invoices shall be raised to TNGB.	Requesting the Bank to clarify to which entity should the invoices of the manpower resources to be billed for endpoint-based solutions (EDR, Asset Management, Patch Management)	It is clarified that the manpower billing shall be raised to TNGB.
60	21	Payment Terms	25. Payment Terms:	25. Payment Terms: Payment Amount on Deliverables Delivery of all the Appliances / Hardware and applicable licenses	Requesting the Bank to kindly consider 100% payment of Device Cost and License Cost upon the delivery of the appliance and applicable license We also request the Bank to consider paying the full GST amount upfront alongwith the first milestone invoice.	Please refer to the amendment. It is clarified that bank is expecting to raise the invoice for only payment due as per payment terms.
61	21	Liquidity Damage	26. LIQUIDATED DAMAGES**Deliverables:**Delivery of all the Appliances/ Hardware/Application Software and applicable licenses	**Liquidity Damage:**0.25% of [A]+[E] for every week's delay or part thereof	Request you not to penalize the bidder on the complete supply value for delays and apply LD on the undelivered portion only. Hence request to amend the clause as follows:" *0.25% of* ***undelivered portion of*** *[A]+[E] for every week's delay or part thereof*"	Please refer to the terms and conditions of the RFP

62	21	Liquidity Damage	26. LIQUIDATED DAMAGES **Deliverables:** Installation and Integration of all Devices and Go-Live of solution, SIGN-OFF	**Liquidity Damage:** 0.50% of [A]+[B]+[E] for every week's delay or part thereof	Request to you to not penalize the bidder on supply items for delay in I&C milestone. Hence request to amend the clause as follows: "0.50% of ~~[A]+[B]+~~[E] for every week's delay or part thereof "	Please refer to the terms and conditions of the RFP
63	22	26. LIQUIDATED DAMAGES	26	 **Deliverables** | **Liquidity Damage** | **Maximum LD** Delivery of all the Appliances/ Hardware/Application Software and applicable licenses | 0.25% of [A]+[E] for every week's delay or part thereof | Up to 10% of (A+B+C+D+E +F) Installation and Integration of all Devices and Go- Live of solution, SIGN-OFF | 0.50% of [A]+[B]+[E] for every week's delay or part thereof	Requesting customer to change maximum LD to 5%	Please adhere to the terms and conditions of the RFP
64	22	Liquidated damages	26. Liquidated damages	Maximum LD to 10%	The Liquidated damages under this section are too stingent increasing the risk exposure of the bidder hence we request you to reduce the Maximum Liquidated Damages to 5%	Please adhere to the terms and conditions of RFP
65	22	General Terms and Condition	Section 5 - General Terms and Conditions on GeM 4.0 (Version 1.12) dt 16th August 2023	5. Contract(s): Following documents shall be construed to be part of the contract generated through GeM: i. Scope of supply including price as enumerated in the Contract Document. ii. General Terms and Conditions (GTC). iii. Product / Service specific Special Terms and Conditions (STC). iv. Product / Track / Domain Specific STC of Particular Service including its SLA (Service Level Agreement) v. Bid / RA specific Additional Terms and Conditions (ATC). **The Terms and Conditions stipulated in STC & SLA will supersede those in GTC and Terms and Conditions stipulated in ATC will supersede those in GTC and STC in case of any conflicting provisions.**	1. Whether document comprising 145 pages **"RfpRRBCSOC_d4141abe-2ac8-4fca-95801693842873951_buyertngbtmd"** to be treated as Additional Terms and Conditions as stated in GEM Bid document? Do we take it that the Additional Terms and conditions forming part of Clause 4 of Gem Document **(Buyer specific ATC)** as the governing document for this RFP? 2. Tata Communications has turnover >500Cr at least in one of the past three completed financial year(s). So, are we exempted from paying EMD of Rs 40 lakhs or not? As per GTC document point **xiii. e-Bidding and Reverse Auction (RA) on GeM - sub clause M** **Note:** No EMD to be taken from exempt category of sellers even by way of specific clauses mentioned in ATC / STC by the Buyers. Such clauses which are against the GeM GTC, will be treated as null and void.	1 - The RFP document mentioned contains all the clauses of RFP. 2 - For availing the exemption from EMD, the company must have turnover > 500 Cr during financial year 2022-23.

66	23	SERVICE LEVEL AGREEMENT (SLA)	27	c) The applicable penalties would be the same irrespective of the root cause.	Any delay not attributable to selected Bidder needs to be taken into consideration and bidder should not be penalized for the same. Hence request to amend the clause as follows: "c) The applicable penalties would be the same irrespective levied after due analysis of root cause. "	Please refer to the amendment
67	23	Man Power	27 (f)	All proposed FM resources as per RFP, must be on the company payroll. Resources from franchise/partners on outsourcing mode are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month (60 Days) notice is required, and Bank's consent is to be obtained.	We request the bank to consider the following. 1) To relax resources being in bidders company payroll. Instead allow resources from franchise / partners approved by the bidder. NTT will take the responsibility wrt statutory requirements like pf, esi, insurance cover etc. 2) Since it is a SLA driven contract, we request the bank to relax the interview process for the resources 3) Our understanding is bank is expecting 60 days notice period only for the outgoing resources. Kindly confirm.	Please adhere to the terms and conditions of RFP for point 1 and 2. For point 3, it is clarified that the understanding is correct.
68	23	Man Power	27. SERVICE LEVEL AGREEMENT (SLA)	All proposed FM resources as per RFP, must be on the company payroll. Resources from franchise/partners on outsourcing mode are not acceptable. All resources should clear interview process by Bank officials/Bank appointed consultants. Before replacing/changing the existing resources, a minimum 2-month (60 Days)notice is required, and Bank's consent is to be obtained	Request to allow subcontracting of L1 Resources.	Please adhere to the terms and conditions of the RFP
69	23	Component failure	a (SLA)	If failure of any supplied component leads to significant downtime more than thrice within a span of six months, then the Bidder has to replace the component or equipment with a similar or higher capable model from the same OEM with the same or higher specifications as mentioned in the RFP at Bidder 's own cost.	To be changed as "If failure of any supplied component leads to significant downtime more than thrice within a span of six months, then the **Bidder/OEM** has to replace the component or equipment with a similar or higher capable model from the same OEM with the same or higher specifications as mentioned in theRFP at Bidder 's own cost."	Please adhere to the terms and conditions of RFP
70	24	Component failure	c (Hardware/Solution Uptime, Group1, Response Time)	Faulty equipment has to be brought up or replacement of same or higher configuration has to be done within 4 hours.	Request bank to change this to NBD replacement as not many OEMs will have a 4 hour replacement option.	It is clarified that Faulty equipment has to be brought up or replacement of same or higher configuration has to be done within 4 hours. If OEM is not having such arrangements, bidder should make necessary

						arrangements to meet the requirements.
71	24	ITSM tool	d (SLA)	The successful bidder has to ensure that the utilisation of resources (Storage, CPU, Memory. RAM, etc) should not exceed 80% of total allocated resource at any time. Alert mechanism to be configured for the threshold limit of 80% so that once it exceeds 80%, alert should be generated and sent to Bank's official.	Does bank have an ITSM tool which can be used to configure the altering and the same can be used by the bidders	It is clarified that till the time bank implements ITSM tool, the alert should be provided manually and on implementation of ITSM, the alert should be generated automatically.
72	24	Hardware / Solution Uptime - Group I	Hardware / Solution Uptime - Group I	Hardware / Solution Uptime - Group I Minimum 99.99% of uptime to be maintained.	Requesting the Bank to move the below mentioned solutions under Group III (Minimum 99.95% of uptime to be maintained): 1. Web Application Firewall 2. Web Proxy with DLP 3.NTP	Please refer to the amendment
73	24	HARDWARE/ SOLUTION UPTIME	I	complete clause	We request Bank to please reduce the penalty as these are at very higher side	Please adhere to the terms and conditions of the RFP
74	25	Penalty	27 - SLA- HW solution uptime	Penalty amount in % will be calculated on Cost of respective solution including AMC/ATS (except Facility Management and Implementation Charges) for 5 years.	We request the bank to exclude the AMC/ATS charges for the penalty calculation.	Please adhere to the terms and conditions of the RFP
75	25	Component failure	9 (Hardware/Solution Uptime, GroupIII, Response Time)	if the central site solution goes down for any reason, solution is expected to come up within 1 hour. During down time redundant site/equipment should be operational. If both sites/HA equipment is down, then penalty will be levied.	Is the bank expecting bidder to factor additional spares for the hardware as the possibilities of both site HA applliances going down would be rare possibilities.	It is clarified that the call to be taken by the successful bidder.
76	26	Mitigation timeline	III) Table-B: Turnaround Time (TAT) for resolution of security Incidents/ Issues	Mitigation timeline	While LTTS shall be responsible to provide the appropriate mitigation steps, respective asset owners / stakeholders from Bank side shall implement or configure the mitigation controls provided by LTTS and LTTS shall provide necessary support to implement the same. Please confirm if our understanding is right.	For the solutions not under scope of the successful bidder, the understanding is right.

77	26	RCA	III) Table-B: Turnaround Time (TAT) for resolution of security Incidents/ Issues	RCA Submission	As per best practices, it is suggested to perform and submit the RCA only for Critical and High Incidents. Please confirm if can consider this revision.	Please adhere to the terms and conditions of the RFP
78	27	Traning to Bank staff	28	The successful bidder shall arrange on premise free training for 2 days for each of the new solution deployed. It should cover complete administration and customization & for day-to-day maintenance of the offered solutions for up to 10 officials of the Bank in Chennai within 1 month after sign-off or before sign-off as per Bank's officer availability. The training should cover all aspects of the solutions solution and should be classroom based.	Our understanding is that Bank wil provide the location for training. Kindly also clarify the following. 1. Is the bank expecting training to be provided by the OEM or the bidder team? 2. Any certification / post training evaluation are expected?	It is clarified that the location of training will be provided by the bank in Chennai. 1) The training is expected to be provided by the OEM. 2) No certification/Post training evaluation are expected.
79	27	Man Power	27 (VI) a	a) The onsite engineer should be available at DC/DR/Any other location as per the shift schedule, irrespective of Holiday of the Bidder company.	Our understanding is that the DC and DR locations for all the 3 banks that are to be supported as part of this RFP is common. Kindly confirm. Kindly share the DC and DR location details.	It is clarified that the DC and DRS locations are common for all the three banks. Location details shall be provided to the successful bidder.
80	27	Man Power	27 (VI) c	The payment for Facility Management/ Onsite Technical Support Resource will be deducted for the number of days of unavailability of the resource. Further penalty of additional Rs.10,000/- (Rupees Ten Thousand only) per resource (L1/L2) per day, as applicable, will be levied for each resource unavailable [if appropriate substitute/replacement of the unavailable resource is not provided].	We request the bank to kindly amend this to INR 5000 per day penalty.	Please adhere to the terms and conditions of the RFP
81	27	Penalty	27 VI (b)	b) Penalty due to absence of any engineer in one quarter will be capped at 100% of the Quarterly FM amount for that resource. e) The successful Bidder has to deploy additional manpower, without any additional cost to the Bank, so as to substitute the off-day, weekly-off, holiday, compensatory off and leave of the L1 resources. Bank will be liable to pay only for the number of resources as mentioned in this RFP or as per the Purchase Order. Further, penalty for the shortfall of Manpower deployed will be levied which will	We would request the bank to clarify the following. 1. The capping on the FMS penalty. The clauses 27VI(b) and 3 (e) are contradicting. Our request is to cap the FMS penalty to 100% of the quarterly FMS charges. 2. For all the resources deployed by the bidder to the bank, kindly allow the resources to follow the banks leave / holiday policy. We also request the bank to share the list of holidays / eligible number of leaves YoY.	Please refer to the amendment. Bank holidays list may be downloaded from Indian bank's website. (i.e) www.indianbank.in

				be additional 20% above the deduction of absence of resources. For L2 resources, leave for 12 days in a year are permitted.		
82	27	Penalty	27. SERVICE LEVEL AGREEMENT (SLA)	The Penalties is limited to maximum of 10% of the total Contract value.	Since separate payment for capex and opex. We request to modify the clause as: a) LD penalty during implementation is limited to maximum of 10% of CAPEX Value v) SLA penalty during AMC is limited to maximum of 10% of OPEX value	Please adhere to the terms and conditions of the RFP
83	28	AMC/ ATS	30 (WARRANTY, ANNUAL MAINTENANCE CHARGES (AMC) & ANNUAL TECHNICAL SUPPORT (ATS)	The period of warranty and subsequent AMC/ATS shall be from the dateof signoff post go-live of all the components of the solution being procured as per RFP.	Request bank to change the signoff to respective solutions, as the solutions which requires agents roll out will have a longer signoff period and other solutions signoff need not be held up.	It is clarified that the signoff pertains to respective solution
84	29	OEM eligibility	Page 29, Section 30 i	The OEM should have a comprehensive known error database or knowledge database in the form a web access which is accessible to Bank team for resolving first level issues. This is not a local database maintained to track incidents. This repository is the knowledge base of all the incidents resolved worldwide by the successful bidder/ OEMs support teams.		* No Query from the bidder.
85	30	Indemnity	34	Indemnity	Tenderer shall indemnify and hold harmless the bidder for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such Bidder.	Please adhere to the terms and conditions of RFP.
86	30	Termination for Convenience	36	Termination of contract for Convenience	1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder up to and including the effective date of the termination of this Agreement. 2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case: a) Its invoices are not paid on time b) If Tenderer fails to comply with the terms of agreement	Please adhere to the terms and conditions of RFP.

87	30	Termination for Convenience	36	Termination of contract for Convenience	Request Bank to remove the clause	Please adhere to the terms and conditions of RFP.
88	30	Indemnity	34. Indemnity	The bidder assumes responsibility for and shall indemnify and keep the Bank harmless from all liabilities, claims, costs, expenses, taxes (except GST) and assessments including penalties, punitive damages, attorney's fees and court costs which are or may be required to be paid by reasons of any breach of the bidder's obligation under these general conditions or for which the bidder has assumed responsibilities under this contract, local or national law or laws, or in respect to all salaries, wages or other compensation to all persons employed/ deployed/services utilized by the bidder or bidders in connection with the performance/ discharge of any system/ obligations covered by the purchase contract. The bidder shall execute, deliver such other further instruments to comply with all the requirements of such laws and regulations as may be necessary there under to confirm and effectuate the purchase contract and to protect the Bank during the tenure of Purchase Order. Where any patent, trademark, registered design, copyrights and/ or intellectual property rights vest in a third party, the bidder shall be liable for settling with such third party and paying any license fee, royalty and/ or compensation, etc., thereon. In the event of any third party raising claim or bringing action against the Bank including but not limited to action for injunction in connection with any rights affecting the solution supplied by the bidder covered under the purchase contract or the use thereof, the bidder agrees and undertakes to defend and / or to assist the Bank in defending at the bidder's cost against such third party's claim and / or actions and against any law suits of any kind initiated against the Bank. Successful bidder will also assume full responsibility of any loss and/or damages, cost, expenses, etc., caused due to malfeasance/misfeasance of any of its	We propose the below mentioned clause :- Each Party shall indemnify the other from and against any claims by third parties (including any Governmental Authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party’s negligence or wilful misconduct.	Please adhere to the Terms and Conditions of the RFP

				solution and/or due to any of their onsite engineer/representative.		
89	30	Termination	36 . Termination for convenience	Either party, by 180 days written notice, may terminate the Contract, in whole or in part, at any time for its convenience.	We propose to include a portion of early termination charges to be paid by TNGB in the event of an early termination by it which shall be equal to fee payable for the term.	It is clarified that charges will be paid for the services availed.
90	30	Price after contract	Exchange rate variation	If the contract is extended for any period, beyond its expiry, the prices shall remain fixed as per the contract signed between the Bank and the Bidder, regardless of variation of exchange rate.	Providing firm price for the extended contract period is very tough, hence we request to modify the clause as: If the contract is extended for any period, beyond its expiry, the prices shall ~~remain fixed as per the contract signed between the Bank and the Bidder~~, be on mutually agreed between Bank and Bidder. And exchange variation on account of this will be mutually agreed basis. ~~regardless of variation of exchange rate.~~	Please refer to the amendment

91	32	Intellectual Property Rights	42. Intellectual Property Rights	42. Intellectual Property Rightsa) The Successful bidder claims and represents that it has obtained all the appropriate rights to provide the Deliverables upon the terms and conditions contained in this contract. The Bank agrees and acknowledges that save as expressly provided in this Contract, all Intellectual Property Rights in relation to the Hardware, Software, Services and Documentation and any adaptations, translations and derivative works thereof, whether protectable as a copyright, trade mark, patent, trade secret design or otherwise, provided by the SECURITY SERVICES Vendor during, in connection with or in relation to fulfilling its obligations under this contract belong to and shall remain a property of the SECURITY SERVICES Vendor or its licensor.	Requesting the Bank to provide more clarity on this clause.We assume that the licenses will be in the name of the Bank, and EULA will be signed between the Bank and the OEMs directly.	IT is clarified that the licenses will be in the name of the bank.
92	32	Intellectual Property Rights	42. Intellectual Property Rights	42. Intellectual Property Rights c) The Successful bidder/ SECURITY SERVICES vendor shall be responsible for obtaining all necessary authorizations and consents from third party licensors of Software/ appliances used by Successful bidder/ SECURITY SERVICES vendor in performing its obligations under this Project.	Requesting the Bank to clarify what authorizations and consents from third party licensors are required.	It is clarified that the successful bidder may contact the respective third party license holders for selling the products to the bank as per this RFP
93	33	Bidder's Liability	43	Limitation of the Bidder's Liability towards the Purchaser	Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	Please adhere to the terms and conditions of RFP.

94	33	Limitation of Liability	43. Limitation of Liability	43. Limitation of Liability h) Any liability/penalty/cost/compensation/charges etc. that cannot be capped or is excluded as a matter of applicable laws and imposed by the statutory authority/ government bodies/court/tribunals etc. in relation to this Contract, owing to the fault of the Successful Bidder/SECURITY SERVICES Vendor.	We see that this is virtually an uncapped liability. Requesting the Bank to cap this liability as well.	Please adhere to the terms and conditions of the RFP
95	33	Limitation of Liability	43. Limitation of Liability	43. LIMITATION OF LIABILITY Successful Bidder's/SECURITY SERVICES Vendor's aggregate liability under the Contract shall be limited to a maximum of the Contract value. For the purposes of this clause, Contract value at any given point of time, means the aggregate value of the purchase orders, paid by Bank to the Successful Bidder/SECURITY SERVICES Vendor that gives rise to claim, under this Contract. In the following circumstances limitation of liability shall not apply and the Successful Bidder/SECURITY SERVICES Vendor shall be liable for amount of cost, damages, compensation, penalty etc. suffered by the Bank: a) Liability of Successful Bidder/SECURITY SERVICES Vendor for third party claims for IP Infringement. b) Liability of Successful Bidder/SECURITY SERVICES Vendor (including third party claims) in case of bodily injury (including Death); c) Liability of Successful Bidder/SECURITY SERVICES Vendor (including third party claims) in case of damage to real property and tangible property caused by the SECURITY SERVICES Vendors' gross negligence. d) Liability of the Successful Bidder/SECURITY SERVICES Vendor in case of gross negligence or wilful misconduct attributable to the Successful Bidder/SECURITY SERVICES Vendor while providing services under this Contract. e) Liability of the Successful Bidder/SECURITY SERVICES Vendor in case of fraudulent acts or wilful misrepresentation attributable to the Vendor regarding the services provided under this Contract.	We propose the below mentioned clause: Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, TC shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent twelve (12) months of charges collected by TC pursuant to the applicable Customer Order Form giving rise to the liability. Nothing in this agreement shall be construed as limiting the liability of either party for (a) personal injury or death resulting from the negligence of a party or its employees, (b) fraud or fraudulent misrepresentation, or (c) wilful misconduct	Please adhere to the terms and conditions of the RFP.

				f) Breach of the confidentiality. g) Employment liabilities for Successful Bidder’s/SECURITY SERVICES Vendor’s staff relating to the period of their employment within contractual period while working with Bank. h) Any liability/penalty/cost/compensation/charges etc. that cannot be capped or is excluded as a matter of applicable laws and imposed by the statutory authority/ government bodies/ court/tribunals etc. in relation to this Contract, owing to the fault of the Successful Bidder/SECURITY SERVICES Vendor.		
96	36	Internal Firewall	1 (Security Solutions Proposed)	Internal Firewalls	Are there any existing firewalls present, which OEM make is that and is there a need for rule migration from existing firewall to the new firewall	It is clarified that rule migration from existing firewall is not required.
97	36	DC/ DR Locations	1. Scope of Work - Security Solutions Proposed	1. Scope of Work - Security Solutions Proposed	Requesting Bank to specify the locations of the DC, DR and other Bank's locations as mentioned in the RFP	It is clarified that the location details will be given to the successful bidder.
98	36	External Firewall	2 (Security Solutions Proposed)	External Firewalls	Are there any existing firewalls present, which OEM make is that and is there a need for rule migration from existing firewall to the new firewall	It is clarified that rule migration from existing firewall is not required.
99	36	DAM	3 (Security Solutions Proposed)	DAM	RFP ask is for 10 DB instances, can the bank share the split of licenses required at DC and DR seperately	It is clarified that the number of licenses are not bound to any location
100	36	DAM	3 (Security Solutions Proposed)	DAM	Bank to clarify in the solution expected on HA at DC and DR	It is clarified that HA is not expected for DAM Solution in DC and DRS
101	36	CLMS	4 (Security Solutions Proposed)	Centralised Log Management Solution (CLMS)	What is the expected EPS count for this solution	Please refer to the RFP page no.84 clause 4.5
102	36	CLMS	4 (Security Solutions Proposed)	Centralised Log Management Solution (CLMS)	Will the bank provide the required Storage (SAN, NAS or other storage types)	It is clarified that the bank will provide required storage
103	36	EDR	5 (Security Solutions Proposed)	Endpoint Detection & Response (EDR)	Will the bank also provide the Enterprise editions of MSSQL or other DB's and also RHEL licenses if required	It is clarified that bank will provide RHEL license. However DB licenses

						need to be arranged by the bidder
104	36	WAF	6 (Security Solutions Proposed)	Web Application Firewall	The SLA requirement is 99.99%, whereas the WAF requirement at DR is on standalone mode, request bank to reduce the SLA and the response time at DR as there are no alternate appliance at the DR site as asked in the RFP.	Please refer to the amendment
105	36	WAF	7 (Security Solutions Proposed)	Web Proxy Solution with Web DLP	Can the solution be proposed on Virtual platform and will the bank provide the required storage. Is the bank expecting the setup to be on HA at DC and DR	It is clarified that the solution can be on virtual platform and bank will provide the required storage. Between DC & DR The bank is not expecting the setup in HA mode within DC or DRS. But it is expected to be in Active-Active mode between DC & DRS.
106	36	SCOPE OF WORK		Bidder to provide new WAF devices with latest features (two at DC) and (One at DRS) as per technical specifications.	We have observed that the bank has used the term DRS , We are assuming that bidder needs to supply and deploy the solution at DC and DR only, please clarify	It is clarified that DR and DRS refer to the same location.
107	37	Asset Management and Patch Management	1	Asset Management - Bidder to provide the Asset management solution for 6500 devices/server and Patch management solution for 5500 devices/Servers and information assets in the bank's network.	Please provide the list of all critical digital assets in scope with the location	It is clarified that the details will be provided to successful bidder.
108	37	SCOPE OF WORK	1.9	1. Scope of Work - Security Solutions Proposed 9. Privileged Identity Management (PIM) Currently, Bank is having similar setup of PIM solution at DC & DRS and currently, Bank is having 50 user licenses which are valid up to 31.07.2024	Please specify the count of devices supported for PIM solution. Does the Bank require Perpetual Based AMC or Subscription Based AMC	Please refer the amendment.
109	37	Centralised/ Any CLMS	1.4 Scope of Work	General	Can we propose one solution for SIEM and Centralised Log Management Solution (CLMS). Or is there any specific requirement to have it as two separate solution.	It is clarified that the choice is left to the bidder.
110	37	DC/ DR Locations	1.A Scope of Work	The Successful bidder/ Security services vendor is responsible for managing the proposed newly deployed solutions (at DC, DR and other Bank's Locations) along with other solutions as	Number of locations to be considered with the split of devices across each location. -Total number of regions [with DC and DR] -Total number of log sources [Servers, Network security devices, EDR, AV, DLP, etc.]	It is clarified that the bidder has to provide the sizing for DC and DR along with the bid.

				per the terms and conditions of this RFP.	-Total number of users. This is important for us to provide the VM Sizing and specifications and the number of VMs required for hosting the log collection agent.	
111	37	VAS	11 (VAS)	Bidder to provide the Vulnerability Assessment Solution for 50 devices concurrently	Is the solution expected only in DC?	It is clarified that the Setup to be configured in one site
112	37	SIEM	8 (Security Solutions Proposed)	Security Incident and Event Management (SIEM)	Will the bank provide the required Storage (SAN, NAS and other storage types) Also, bank to clarify if the solution is expected to be in HA at DC and DR	It is clarified that Bank will provide the required storage. Please refer to RFP page no. 65 and clause no.58 for HA requirements.
113	37	PIM	9 (Privilege Identity management (PIM)	The solution to be configured to be used as AA Solution for non-critical devices.	We presume this is AAA and not AA, also kindly mention what are these non-critical devices	It is clarified that AA is the requirement. Bidder may provide AAA.
114	37	PIM	9 (Privilege Identity management (PIM)	The solution should be scalable for future expansion and needs.	As the solution is already deployed at the bank, please clarify if the existing platform is scalable for future expansion.	Yes, the existing solution is scalable.
115	37	PIM	Section 3., Scope of Work	Currently, Bank is having similar setup of PIM solution at DC & DRS and currently, Bank is having 50 user licenses which are valid up to 31.07.2024	Currently 50 users and 500 device licenses are there, do we need to consider the additional 500 device licenses.	Please refer the amendment.
116	38	Security Audit frequency	1. SCOPE OF WORK	(j) Successful bidder/ Security services vendor has to ensure remediation of the Security Audit/ Third party audit observations on security devices/ solutions under scope of this RFP.	Please confirm the frequency of security Audit / Third Party that shall happen Year on Year. This will help us to factor the required efforts and support form our side.	It is clarified that the frequency of security Audit / Third Party shall happen half yearly subject to the regulatory guidelines and bank's policy from time to time.
117	38	Connectivity	1.E Scope of Work	Bidder has to submit implementation plan and the details of plan should not be limited to Architecture Diagram, low level detailed network diagram considering the interfaces, peer connectivity, RACK & Floor details, etc along with project schedule date for deployment of new security solutions proposed as per this RFP.	Is there interconnectivity between the locations/sites? If so, what kind of connectivity	It is clarified that the interconnectivity between locations/sites available with P2P and MPLS links.

118	38	Report generation	Scope of work 1 (N)	a) Bidder has to provide reports for all the solutions on a daily basis for executive reporting in addition to the detailed reports. Some of the reports may be required multiple times in a day. Bank may also ask customised reports of any solution based on Bank's requirement and same has to be provided.	Our understanding is that the reports that are customizable through the consoles provided by OEMs of the various solutions is what is expected by the bank. Custom development for report generation is out of scope. Kindly confirm.	It is clarified that bidder has to provide the customized reports through the OEM console.
119	39	SCOPE OF WORK	1-p	Only after successful running of solutions for one-month period, the solutions will be taken over by successful bidder's facility management/ onsite support engineers for providing further services as per scope of work of this RFP document	Bank to clarify from when the operation team be onboarded and from when does the contract period starts.	Please refer to the amendment
120	39	SCOPE OF WORK	1-p	Only after successful running of solutions for one-month period, the solutions will be taken over by successful bidder's facility management/ onsite support engineers for providing further services as per scope of work of this RFP document	We request Bank to please reduce the monitoring time from one month to 15 days and also assuming that bidder need to provide the FMS from the date of acceptance kindly confirm	Please refer to the amendment
121	39	Man Power	2.ONSITE TECHNICAL SUPPORT (FACILITY MANAGEMENT SERVICES)]	The successful Bidder has to provide onsite technical support [Facility Management Services] resources for maintenance and monitoring of the new and existing solutions for a period of five (5) years as per scope of this RFP and provide AMC/ATS as applicable for the solutions as per the technical specifications.	Please clarify on the below 1. Does the bank expect the bidder to provide 24x7 for device management as well. 2. Can the device management scope be performed remotely or should we have the resources deployed onsite. 3. If it has to be onsite, the number of resources [L1 and L2] has to be increased as per the scope.	1.Device management is expected from 08:00 AM to 08:00 PM. If the device is down, the engineer is to attend the call 24X7 2.The device management is to be carried out onsite only 3.Please refer to the amendment
122	39	Man Power	Onsite Technical Support (Facility Management Services)	Onsite Technical Support (Facility Management Services) Onsite Technical resource will also have to manage the existing security solution/components/devices already deployed by the Bank as well as new solutions under the scope of this RFP	We assume this is a green-field project. Incase of any existing devices, kindly share the device inventory.	It is clarified that the existing device inventory will be provided to the successful bidder.

123	39	SIEM	s (Scope of Work)	All the solutions have to be integrated in SIEM as well as in Syslog servers for necessary system logs before Signing-Off the respective solutions. The Bank will verify that the proper log details are being received by the SIEM and Syslog Server or not	Can bank provide the number of applications that needs to be integrated with the SIEM tool so that we can factor the number of custom parsers accordingly.	All Information Security Solutions procured through this RFP, Servers and Authentication systems should be integrated on installation of SIEM tool. Any other solutions procured by bank subsequently need to be integrated with the SIEM when required.
124	39	DR drill support	Scope of work 1 (W)	a) The successful Bidder has to provide necessary support during DR Drill, Cyber Drill or any other such activity undertaken by the Bank.	Kindly confirm the frequency of the DR / Cyber drills expected by the bank. Will this be common for all the 3 banks or each bank can request for independent DR/Cyber drills?	It is clarified that the frequency of DR drill/Cyber drill will be at least half yearly once.
125	39	Logs	u (Scope of Work)	Bidder has to take necessary periodic backup like Configuration, logs etc as per bank's policy.	Will the bank provide the necessary backup solution and storage for this?	It is clarified that the storage will be provided by the bank. The bidder should consider the tools required for meeting the RFP requirement.
126	40	REQUIREMENT OF MAN POWER	3	L3 resource (On call support – Should be available onsite whenever required)	we request bank to please share the time lines to provide the on site l3 resource	It is clarified that L3 support is required from the date of commencement of operations
127	40	Man Power	3. Requirement of Man Power	3. Requirement of Man Power	Requesting Bank to clarify if the proposed count of L1, L2 and L3 resources are only for supporting device management of the security devices (or) also for supporting SIEM Operations & Engineering. If the resources are also to support SIEM Operations & Platform, suggesting the Bank to increase the count of resources as below: L1 - 3 seats (24x7x365) L2 - 5 resources (2 for SIEM Engineering & 3 for Security Device Management) L3 - 2 resources dedicated onsite	It is clarified that the resources should manage security devices and also support SIEM operations. Please refer amendment for the change in resource count.

128	40	Man Power	3. REQUIREMENT OF MAN POWER	L1 onsite resource at DC/DR/ Other Locations as specified by Bank L2 onsite resource at DC/DR Other Locations as specified by Bank L3 resource (On call support – Should be available onsite whenever required)	Kindly confirm the locations and the count of the total L1 & L2, to estimate the manpower effort charges. Further request to include the off-site L3 resource also in BOQ under TABLE- C	Location details shall be provided to the successful bidder. For other queries, please adhere to the terms and conditions of the RFP.
129	40	Man Power	3. Requirement of Man Power L2 resource will be working as per Bank's working day in Chennai except emergency requirements.	3. Requirement of Man Power L2 resource will be working as per Bank's working day in Chennai except emergency requirements.	Please specify Bank working days and working hours	It is clarified that L2 resources should work from 0800 hrs to 2000 hrs in shift. Bank holidays list may be downloaded from Indian bank's website. (i.e) www.indianbank.in.
130	40	Man Power	3.REQUIREMENT OF MAN POWER	Man Power Requirement	can we deploy rest of the L1 resources remotely. For the scope of work considered, including device management it would be difficult to manage with 1 L1 resource onsite.	Please refer to the amendment.
131	40	Incident reporting	Onsite technical support 1 (D)	a) The successful Bidder should ensure reporting any incident & take approval from bank in writing to remediate the incident immediately.	We request the bank to relax taking written approval from bank for incident remediation. This is because for critical incidents immediate action will be required. However the bidder can keep the bank stakeholders informed about the incidents and also provide RCA.	It is clarified that the emergency execution route defined in the bank policy to be followed in case of critical incidents which need immediate action.
132	40	DC/ DR Locations	REQUIREMENT OF MAN POWER	L1, L2 resources at DC/DR/Other locations	Kindly provide the DC/DR/Other locations.	Location details shall be provided to the successful bidder
133	40	Man Power	Requirement of man power (S.No 1)	L1 onsite resource at DC/DR/ Other Locations as specified by Bank - 1 seat	Is it 1 seat in DC and 1 seat in DR. Kindly confirm. Also, 1 seat would mean 1 resource per shift. Considering the complexity / count of the solutions and the and the regular tasks to be performed we would recommend 6 L1 resources in each shift (2 resources for each group) . We request the bank to kindly consider the same.	It is clarified that the L1 seat will be in any one location of DC/DRS/any location provided by the bank. Please refer to the amendment for additional resources.
134	40	Man Power	Requirement of man power (S.No 1)	L3 resource (On call support – Should be available onsite whenever required	Instead of Oncall support for L3, we request the bank to consider 1 dedicated L3 resoruce during the bank working days Onsite in the DC of the bank. Kindly confirm. Additionally, to manage the entire operations one dedicated Team leader / Service delivery manager also to be factored. We	Please adhere to the terms and conditions of the RFP

					request the bank to kindly include provide provision for this resource also in the RFP.	
135	40	Man Power	Requirement of man power (S.No 2)	L2 onsite resource at DC/DR Other Locations as specified by Bank - 3.	Kindly confirm if 3 is the total number of resoruces to be deployed or the count of seats. Also pls confirm the service window for the L2 resources. Our recommendation is to have one L2 resource in each shift for each group.	It is clarified that 3 number of resources to be deployed. Normally, shift time for L2 resources will be 08:00 to 20:00 hrs.
136	41	Penalty	3 (e)	Further, penalty for the shortfall of Manpower deployed will be levied which will be additional 20% above the deduction of absence of resources. For L2 resources, leave for 12 days in a year are permitted.	We would request the bank to clarify the following. 1. The capping on the FMS penalty. The clauses 27VI(b) and 3 (e) are contradicting. Our request is to cap the FMS penalty to 100% of the quarterly FMS charges. 2. For all the resources deployed by the bidder to the bank, kindly allow the resources to follow the banks leave / holiday policy. We also request the bank to share the list of holidays / eligible number of leaves YoY.	Please refer the amendment.
137	41	REQUIREMENT OF MAN POWER		The successful Bidder has to deploy additional manpower, without any additional cost to the Bank, so as to substitute the off-day, weekly-off, holiday, compensatory off and leave of the L1 resources. Bank will be liable to pay only for the number of resources as mentioned in this RFP or as per the Purchase Order. Further, penalty for the shortfall of Manpower deployed will be levied which will be additional 20% above the deduction of absence of resources. For L2 resources, leave for 12 days in a year are permitted.	Bank has asked for 9 resources which include 3-L1, 3-L2, and 1-L3 in the general shift. But based on the statement made on page 41, point E, it seems the bank has intended to run operation 24x7x365 which may require more resources. Please share the exact count. As both points are contradictory	Please refer to the amendment. L1 resource for 24*7*365 shift is for 1 seat which may need to be staffed as per successful bidder's company policy.
138	43	Man Power	4. Individual Roles and Responsibilities of Onsite and Oncall Technical Support Resources Level 3 Support y) Carry out cyber risk assessment for Bank quarterly & recommend risk mitigation measures in the monthly review meetings.	4. Individual Roles and Responsibilities of Onsite and Oncall Technical Support Resources Level 3 Support y) Carry out cyber risk assessment for Bank quarterly & recommend risk mitigation measures in the monthly review meetings.	Requesting the Bank to clarify what kind of cyber risk assessment is expected to be carried by the L3 resource, as this is a service by itself.	It is clarified that Cyber risk assessment to be done based on the risk identified.

139	44	Man Power	5. Requirement of Manpower Skillset Level-1 (L1) Minimum 3 years of experience in handling security related products & services in scope	5. Requirement of Manpower Skillset Level-1 (L1) Minimum 3 years of experience in handling security related products & services in scope	Requesting the Bank to change this clause as: "Minimum 2-3 years of experience in handling security related products & services in scope"	Please adhere to the terms and conditions of the RFP
140	44	Man Power	5. Requirement of Manpower Skillset Level-2 (L2) Minimum overall 5 years of experience in handling security related products	5. Requirement of Manpower Skillset Level-2 (L2) Minimum overall 5 years of experience in handling security related products	Requesting the Bank to change this clause as: "Minimum overall 3-5 years of experience in handling security related products"	Please adhere to the terms and conditions of the RFP
141	44	Man Power	Requirement of Manpower skill set	L2 / L3: Educational qualification: B.E. /B.Tech or above in Computer Science/Electronics/IT/Electrical Engineering/ MCA.	We request the bank to relax the B.E / B.Tech for the L2/L3 resources. This will support to promote the L1 to the L2/L3 team. (For L1 BSc/Diploma is allowed).	Please adhere to the terms and conditions of the RFP
142	44	Man Power	**SECTION 3 - SCHEDULE OF REQUIREMENTS** (SECTION 3 - SCHEDULE OF REQUIREMENTS)	Position: Level-1 (L1) BSc /Diploma or above in Computer Science/Electronics/IT/Electrical Engineering.	**Request you to modify this clause as:** BSc /**BCA**/Diploma in Computer Science/Electronics/IT/Electrical Engineering.	Please refer to the amendment
143	44	Man Power	**SECTION 3 - SCHEDULE OF REQUIREMENTS**(SECTION 3 - SCHEDULE OF REQUIREMENTS)	Position: Level-1 (L1)Minimum Cost To Company(CTC) expected for the L1 resource is 6 Lakhs perannum.	**Request you to remove the clause as:**The CTC clause of all the organization is based on their terms and conditions, and policies, hence, this should be in the prerogative of the bidder and such restriction may be removed to allow open and wider participation.	It is clarified that the minimum CTC is only mentioned in the RFP to have quality resources. However bidder may offer salary above this.

144	44	Man Power	**SECTION 3 - SCHEDULE OF REQUIREMENTS** (SECTION 3 - SCHEDULE OF REQUIREMENTS)	Position: Level-2 (L2) Minimum overall 5 years of experience in handling security related products & services out of which 3 years' experience should be in SIEM/ Firewall /WAF/ DAM.	**Request you to modify this clause as:** Minimum overall 5 years of experience in handling security related products & services out of which **02 years** experience should be in SIEM/ Firewall /WAF/ DAM. **Request to add certification like ISO 27001 Certification or Professional/Advance level OEM certification like CCNP, NSE , etc.**	Please adhere to the terms and conditions of the RFP
145	44	Man Power	**SECTION 3 - SCHEDULE OF REQUIREMENTS** (SECTION 3 - SCHEDULE OF REQUIREMENTS)	Position: Level-3 (L3) Minimum 10 years of experience in handling security related products & services in an organization and out of total experience, 5 years of minimum experience should be as an L2 in SOC management.	**Request you to modify this clause as:** Minimum 10 years of experience in handling security related products & services in an organization and out of total experience, **03 years** of minimum experience should be as an L2 in SOC management.	Please adhere to the terms and conditions of the RFP
146	45	Man Power	5. Requirement of Manpower Skillset Level-3 (L3) At least one security certifications CCIE/CISSP/CISA/ CISM	5. Requirement of Manpower Skillset Level-3 (L3) At least one security certifications CCIE/CISSP/CISA/CISM	Requesting the Bank to change this clause as: "At least one security certifications CCIE/CISSP/CISA/CISM/CEH/CCNP"	No change. Please adhere to the terms and conditions of the RFP
147	45	SIEM	Microfocus - SIEM	The solution must provide near-real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis.	Near-real time alerting pose a significant security risk to bank, hence requesting to modify as "The solution must provide real time correlation alerting of events. "	Please adhere to the terms and conditions of the RFP
148	45	SIEM	SIEM	The solution must provide near-real-time analysis of events. Mention lag, if any, between the actual event and its reporting with analysis.	Near-real time alerting pose a significant security risk to bank, hence requesting to modify as "The solution must provide real time correlation alerting of events. "	Please adhere to the terms and conditions of the RFP
149	46	DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS	6	Within 8 weeks from date of PO acceptance	We request Bank to please provide the 12 weeks for the all hardware delivery and 4 weeks for the installation	Please adhere to the terms and conditions of the RFP

150	46	Delivery Timelines	6. Delivery and Implementation Timelines of the Solutions Delivery of Hardware / Appliance / Licenses at respective locations	6. Delivery and Implementation Timelines of the Solutions Delivery of Hardware / Appliance / Licenses at respective locations	Requesting the Bank to increse the Delivery Timelines to 12 weeks from the date of PO acceptance	Please adhere to the terms and conditions of the RFP
151	46	Delivery Timelines	6. Delivery and Implementation Timelines of the Solutions Implementation / Integration / Go-Live / Sign-off at respective locations	6. Delivery and Implementation Timelines of the Solutions Implementation / Integration / Go-Live / Sign-off at respective locations	Requesting the Bank to increse the Implementation Timelines to 16 weeks from the date of PO acceptance. Agents roll-out will be part of Operations phase.	Please adhere to the terms and conditions of the RFP
152	46	Delivery Timelines	6. DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS:	6. DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS:	Due to global chip shortage, shortage of raw materials after pandemic, delivery of Hardware/ Appliance/ Licenses at respective site locations in 8 weeks time is very challenge. hence we request to amend the clause as follow: Delivery Hardware/ Appliance/ Licenses at respective site locations : Within ~~8~~ 15 weeks from date of PO acceptance Implementation/ Integration/Go Live/ Sign-Off at respective locations: Within ~~10~~ 18 weeks from date of PO acceptance Commencement of Facility Management Services at respective locations: Within ~~90~~ 21 weeks from date of PO acceptance	Please adhere to the terms and conditions of the RFP
153	46	Delivery Timelines	DELIVERY AND IMPLEMENTATION TIMELINES OF THE SOLUTIONS	All the solutions	Request bank to extend the hardware delivery by additional 2 weeks and implementation and sign-off by another 2 weeks for all the solutions	Please adhere to the terms and conditions of the RFP

154	46	Delivery Timelines	Delivery and Implementation timelines of the solutions	Delivery of Hardware/ Appliance/ Licenses at respective locationsInternal Firewall, External Firewall, Web Application Firewall, Security Incident and Event Management (SIEM) - Within 8 weeks from date of PO acceptance Database Activity Monitoring(DAM) Solution, Centralised Log Management Solution (CLMS),Web Proxy Solution with Web DLP - Within 4 weeks from date of PO acceptance	Considering the project complexitiies and increased resource commitment, Kindly revise the delivery terms as belowInternal Firewall, External Firewall, Web Application Firewall, Security Incident and Event Management (SIEM) - Within 12 weeks from date of PO acceptance Database Activity Monitoring(DAM) Solution, Centralised Log Management Solution (CLMS),Web Proxy Solution with Web DLP - Within 8 weeks from date of PO acceptance	Please adhere to the terms and conditions of the RFP
155	46	Delivery Timelines	Delivery and Implementation timelines of the solutions	Implementation/ Integration/Go Live/ Sign-Off at respective locations Internal Firewall, External Firewall, Web Application Firewall, - Within 10 weeks from date of PO acceptance Security Incident and Event Management (SIEM) - Within 12 weeks from date of PO acceptance Database Activity Monitoring(DAM) Solution, Centralised Log Management Solution (CLMS),- Within 5 weeks from date of PO acceptance Web Proxy Solution with Web DLP - Within 8 weeks from date of PO acceptance Endpoint Detection & Response(EDR) - Within 16 weeks from date of PO acceptance	Considering the project complexitiies and increased resource commitment, Kindly revise the delivery terms as belo Internal Firewall, External Firewall, Web Application Firewall, - Within 14 weeks from date of PO acceptance Security Incident and Event Management (SIEM) - Within 16 weeks from date of PO acceptance Database Activity Monitoring(DAM) Solution, Centralised Log Management Solution (CLMS),- Within 9 weeks from date of PO acceptance Web Proxy Solution with Web DLP - Within 12 weeks from date of PO acceptance Endpoint Detection & Response(EDR) - Within 20 weeks from date of PO acceptance	Please adhere to the terms and conditions of the RFP
156	48	SIEM	Microfocus - SIEM	Solution should support at least rule based, nonrule based, vulnerability based and statistical based correlation	Please clarify the use case for nonrule based correlation	It is clarified that when SIEM detects a deviation in behavior of logs received, based on threat intelligence and other anomaly detection intelligence available in the SIEM alert to be triggered.

157	48	SIEM	SIEM	Solution should support at least rule based, nonrule based, vulnerability based and statistical based correlation	Please clarify the use case for nonrule based correlation	It is clarified that when SIEM detects a deviation in behavior of logs received, based on threat intelligence and other anomaly detection intelligence available in the SIEM alert to be triggered.
158	49	Internal Firewall	10. Internal Firewall	The Firewall solution should facilitate compliance to GDPR, PCI DSS, SOX, ISO 27001 and SOC 2 requirements.	Please clarify if Product should be complied above standards or if feature is required to show above compliance violations in policies	It is clarified that the feature is required to show the compliance violations in policies.
159	49	Internal Firewall	10. Internal Firewall	The Firewall solution should facilitate compliance to GDPR, PCI DSS, SOX, ISO 27001 and SOC 2 requirements.	Please clarify if Product should be complied above standards or if feature is required to show above compliance violations in policies	It is clarified that the feature is required to show the compliance violations in policies.
160	49	Internal Firewall	10. Internal Firewall	The Firewall solution should facilitate compliance to GDPR, PCI DSS, SOX, ISO 27001 and SOC 2 requirements.	Please clarify if Product should be complied above standards or if feature is required to show above compliance violations in policies	It is clarified that the feature is required to show the compliance violations in policies.
161	49	Internal Firewall	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 10: The Firewall solution should facilitate compliance to GDPR, PCI DSS, SOX, ISO 27001 and SOC 2 requirements.	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 10: The Firewall solution should facilitate compliance to GDPR, PCI DSS, SOX, ISO 27001 and SOC 2 requirements.	Please clarify if Product should be complied above standards or if feature is required to show above compliance violations in policies	It is clarified that the feature is required to show the compliance violations in policies.

162	50	Internal Firewall	16. Internal Firewall	The Firewall solution should be loaded with maximum memory modules feasible. Each Memory module should have maximum memory	Please specify the memory required, as different OEM's would have different sizing parameters	It is clarified that the maximum memory modules feasible in the particular firewall solution should be fully loaded.
163	50	Internal Firewall	16. Internal Firewall	The Firewall solution should be loaded with maximum memory modules feasible. Each Memory module should have maximum memory	Please specify the memory required, as different OEM's would have different sizing parameters	It is clarified that the maximum memory modules feasible in the particular firewall solution should be fully loaded.
164	50	Internal Firewall	16. Internal Firewall	The Firewall solution should be loaded with maximum memory modules feasible. Each Memory module should have maximum memory	Please specify the memory required, as different OEM's would have different sizing parameters	It is clarified that the maximum memory modules feasible in the particular firewall solution should be fully loaded.
165	50	Internal Firewall	21. Internal Firewall	The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	10G and 1G will be used for uplink and Downlink hence 10 no's of Ethernet is not required. Please reduce the count to 8	Please refer to the amendment
166	50	Internal Firewall	21. Internal Firewall	The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	10G and 1G will be used for uplink and Downlink hence 10 no's of Ethernet is not required. Please reduce the count to 8	Please refer to the amendment
167	50	Internal Firewall	21. Internal Firewall	The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	10G and 1G will be used for uplink and Downlink hence 10 no's of Ethernet is not required. Please reduce the count to 8	Please refer to the amendment

168	50	Internal Firewall	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 16: The Firewall solution should be loaded with maximum memory modules feasible. Each Memory module should have maximum memory	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 16: The Firewall solution should be loaded with maximum memory modules feasible. Each Memory module should have maximum memory	Please specify the memory required, as different OEM's would have different sizing parameters	It is clarified that the maximum memory modules feasible in the particular firewall solution should be fully loaded.
169	50	Internal Firewall	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 21: The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	Section 4 - Specifications and Allied Technical Details 1. Internal Firewall - Point 21: The other physical ports should be- 10 nos. of 1G Copper Ethernet, 4 nos. of 1G fiber 4 nos. of 10G SFP+	10G and 1G will be used for uplink and Downlink hence 10 no's of Ethernet is not required. Please reduce the count to 8.	Please refer to the amendment
170	52	Internal Firewall	53. Internal Firewall	Appliance must have minimum 32 GB of RAM and 240 GB storage. RAM should be upgradable up to 128GB	Point 16 is contradicting the current point. Please clarify. Additionally, its sufficient to have 64 GB for internal firewall. Please scale down the max memory to 64GB	No change

171	52	Internal Firewall	53. Internal Firewall	Appliance must have minimum 32 GB of RAM and 240 GB storage. RAM should be upgradable up to 128GB	Point 16 is contradicting the current point. Please clarify. Additionally, its sufficient to have 64 GB for internal firewall. Please scale down the max memory to 64GB	No change
172	52	Internal Firewall	53. Internal Firewall	Appliance must have minimum 32 GB of RAM and 240 GB storage. RAM should be upgradable up to 128GB	Point 16 is contradicting the current point. Please clarify. Additionally, its sufficient to have 64 GB for internal firewall. Please scale down the max memory to 64GB	No change
173	52	Internal Firewall	Section 4 - Specifications and Allied Technical Details1. Internal Firewall - Point 53:Appliance must have minimum 32 GB of RAM and 240 GB storage. RAM should be upgradable up to 128GB	Section 4 - Specifications and Allied Technical Details1. Internal Firewall - Point 53:Appliance must have minimum 32 GB of RAM and 240 GB storage. RAM should be upgradable up to 128GB	Point 16 (mentioned above) is contradicting with the current point. Please clarify. Additionally, it is sufficient to have 64 GB for internal firewall.Please scale down the max memory to 64GB.	No change
174	54	External Firewall	81 (External Firewall)	Existing Clause : The throughput of the Firewall solution should be minimum 1 Gbps after enabling NIPS, Anti-APT, sandboxing, Logging etc. with recommended secured algorithms during the contract period.	Requested Change : The Threat Prevention throughput of Firewall Solution should be minimum 3 Gbps after enabling NIPS,Anti-APT,Sandboxing,Logging,Reporting etc for packet size of 64 KB. Justification: This clause is conflicting with clause 117. Recommendation is to merge them into single clause.Threat Prevention Throughput should be measured with NIPS,Anti-APT,Sandboxing,Logging,Reporting enabled. As the Firewall solution is expected to function with all security features and logging capabilities since day 1. The modified clause clearly specifies the desired threat prevention throughput and also mentions that the throughput is measured for the smallest packet size i.e 64kb	Please refer to the amendment

175	54	External Firewall	External Firewall	Existing Clause : The throughput of the Firewall solution should be minimum 1 Gbps after enabling NIPS, Anti-APT, sandboxing, Logging etc. with recommended secured algorithms during the contract period.	Requested Change : The Threat Prevention throughput of Firewall Solution should be minimum 3 Gbps after enabling NIPS,Anti-APT,Sandboxing,Logging,Reporting etc for packet size of 64 KB. Justification: This clause is conflicting with clause 117. Recommendation is to merge them into single clause.Threat Prevention Throughput should be measured with NIPS,Anti-APT,Sandboxing,Logging,Reporting enabled. As the Firewall solution is expected to function with all security features and logging capabilities since day 1. The modified clause clearly specifies the desired threat prevention throughput and also mentions that the throughput is measured for the smallest packet size i.e 64kb	Please refer to the amendment
176	54	External Firewall	Section 4 - Specifications and Allied Technical Details 2. External Firewall - Point 81: The throughput of the Firewall solution should be minimum 1 Gbps after enabling NIPS, Anti-APT, sandboxing, Logging etc. with recommended secured algorithms during the contract period.	Section 4 - Specifications and Allied Technical Details 2. External Firewall - Point 81: The throughput of the Firewall solution should be minimum 1 Gbps after enabling NIPS, Anti-APT, sandboxing, Logging etc. with recommended secured algorithms during the contract period.	This clause is conflicting with clause 117. Requesting the Bank to merge both these clauses into a single clause as below: The Threat Prevention throughput of Firewall Solution should be minimum 3 Gbps after enabling NIPS, Anti-APT, Sandboxing, Logging, Reporting etc for packet size of 64 KB	Please refer to the amendment
177	55	External Firewall	92	Existing Clause : The Firewall solution should support operation modes- Active\Active, Active\Standby and Clustering (for scalability).	Requested Change : The Firewall solution should support operation modes- Active\Active, Active\Standby Justification : Clustering is an OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications	It is clarified that if clustering is not available appropriate HA technology to be implemented.

178	55	External Firewall	92	Existing Clause : The Firewall solution should support operation modes- Active\Active, Active\Standby and Clustering (for scalability).	Requested Change : The Firewall solution should support operation modes- Active\Active, Active\Standby Justification : Clustering is an OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications	It is clarified that if clustering is not available appropriate HA technology to be implemented.
179	55	External Firewall	92	Existing Clause : The Firewall solution should support operation modes- Active\Active, Active\Standby and Clustering (for scalability).	Requested Change : The Firewall solution should support operation modes- Active\Active, Active\Standby Justification : Clustering is an OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications	It is clarified that if clustering is not available appropriate HA technology to be implemented.
180	56	External Firewall	106	The firewall should not connect to public\vendor cloud for any of its functions	Request for Deletion of Existing Clause : The firewall should not connect to public\vendor cloud for any of its functionsJustification : Today's cyberattacks are becoming increasingly sophisticated. Attackers are using the latest techniques target organizations. To protect against these threats, firewalls need to be able to use the latest technologies as well. The firewall being the first line of defense should have the capabilities to use AI,ML capabilities and leverage Cloud based analysis and compute to protect your network against unknown and evasive threats.	It is clarified that connection to OEM cloud should be only for receiving the threat intelligence update at periodic intervals.
181	56	SIEM	SIEM	The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier.	The requested usecases are addressed through the packet capture solution, requesting to remove the point as it is mentioned in point 80 to not provide NTA or NBAD solution as a part of this bid	Please adhere to the terms and conditions of the RFP

182	56	SIEM	SIEM	The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier.	The requested usecases are addressed through the packet capture solution, requesting to remove the point as it is mentioned in point 80 to not provide NTA or NBAD solution as a part of this bid	Please adhere to the terms and conditions of the RFP
183	57	External Firewall	107	The firewall should not connect to public\vendor cloud for any of its functions	Request for Deletion of Existing Clause : The firewall should not connect to public\vendor cloud for any of its functions Justification : Today's cyberattacks are becoming increasingly sophisticated. Attackers are using the latest techniques target organizations. To protect against these threats, firewalls need to be able to use the latest technologies as well. The firewall being the first line of defense should have the capabilities to use AI,ML capabilities and leverage Cloud based analysis and compute to protect your network against unknown and evasive threats.	It is clarified that connection to OEM cloud should be only for receiving the threat intelligence update at periodic intervals.
184	57	External Firewall	117	Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput	Request of deletion of Duplicate Clause : Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput Justification : This clause is conflicting with clause 81. As stated above we can merge both the clauses into one single clause and delete this duplicate clause.	Please refer to the amendment
185	57	External Firewall	117	Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput	Request of deletion of Duplicate Clause : Proposed firewall appliance should support minimum of 3.5Gbps of Threat prevention throughput Justification : This clause is conflicting with clause 81. As stated above we can merge both the clauses into one single clause and delete this duplicate clause.	Please refer to the amendment

186	57	External Firewall	118	Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1	Request for Deletion of Existing Clause : Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1 Justification: Clustering is OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications. If a higher threat prevention throughput is required, please explain why 20 Gbps is needed.The percentage increase from the requirement in Clause 81 (1 Gbps) to 20 Gbps is extremely high and not justifiable.Also The throughput of internal firewall is only 6 Gbps which includes both east west and north south traffic, considering this we ask you to remove this clause from the RFP.	Please refer to the amendment
187	57	External Firewall	118	Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1	Request for Deletion of Existing Clause : Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1 Justification: Clustering is OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications. If a higher threat prevention throughput is required, please explain why 20 Gbps is needed.The percentage increase from the requirement in Clause 81 (1 Gbps) to 20 Gbps is extremely high and not justifiable.Also The throughput of internal firewall is only 6 Gbps which includes both east west and north south traffic, considering this we ask you to remove this clause from the RFP.	Please refer to the amendment
188	57	External Firewall	118	Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1	Request for Deletion of Existing Clause : Proposed firewall should be able to scale up to 20Gbps of threat prevention throughput in future if required by adding additional hardware in to the existing cluster to meet the future growth or the same can be supplied from Day-1 Justification: Clustering is OEM specific Framework and will restrict other leading OEMs to participate in the RFP specifications. If a higher threat prevention throughput is required, please explain why 20 Gbps is needed.The percentage increase from the requirement in Clause 81 (1 Gbps) to 20 Gbps is extremely high and not justifiable.Also The throughput of internal firewall is only 6 Gbps which includes both east west and north south traffic, considering this we ask you to remove this clause from the RFP.	Please refer to the amendment

189	57	External Firewall	123	Existing Clause : Appliance must have minimum 32 GB of RAM, minimum 12 physical cores and 240 GB storage. RAM Should be upgradable up to 128 GB	Requested Change : The Appliance must have minimum 8 physical cores and 120 Gb storage. Justification : The performance of a firewall appliance is primarily determined by the number of cores, hardware architecture, and software. The amount of RAM only affects the number of sessions that the firewall can handle. Since the session requirement is specified in a different clause, the RAM requirement here is redundant. Additionally, since logging, reporting, and management will be handled by a separate dedicated device, 120 GB of storage is sufficient for the appliance. The RAM scalability requirement is specific to a particular OEM architecture and should be removed.	Please refer to the amendment
190	57	External Firewall	123	Existing Clause : Appliance must have minimum 32 GB of RAM, minimum 12 physical cores and 240 GB storage. RAM Should be upgradable up to 128 GB	Requested Change : The Appliance must have minimum 8 physical cores and 120 Gb storage.Justification : The performance of a firewall appliance is primarily determined by the number of cores, hardware architecture, and software. The amount of RAM only affects the number of sessions that the firewall can handle. Since the session requirement is specified in a different clause, the RAM requirement here is redundant. Additionally, since logging, reporting, and management will be handled by a separate dedicated device, 120 GB of storage is sufficient for the appliance. The RAM scalability requirement is specific to a particular OEM architecture and should be removed.	Please refer to the amendment
191	58	External Firewall	108	The firewall should not connect to public\vendor cloud for any of its functions	Request for Deletion of Existing Clause : The firewall should not connect to public\vendor cloud for any of its functions Justification : Today's cyberattacks are becoming increasingly sophisticated. Attackers are using the latest techniques target organizations. To protect against these threats, firewalls need to be able to use the latest technologies as well. The firewall being the first line of defense should have the capabilities to use AI,ML capabilities and leverage Cloud based analysis and compute to protect your network against unknown and evasive threats.	It is clarified that connection to OEM cloud should be only for receiving the threat intelligence update at periodic intervals.

192	58	External Firewall	External Firewall	Existing Clause : Reports on risk analysis of firewall rules based on bank’s own current Risk Matrix which will learn and develop on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc.	Modified Clause: Reports on Best practice assessment of firewall rules based on OEMs Risk Matrix as well as industry standards such as CIS checks which will learn and about rules on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc. Justification: Every OEM has their own analytics engine/dashboard metrics. Our platform can provide detailed information around Best practice assesment and feature adoption for rules in the deployed enviroment. It also perform checks against industry standards such CIS.This ensures that the security rules are configured in the best way possible.	It is clarified that OEM's risk matrix customizable to bank's risk matrix is accepted.
193	58	External Firewall	External Firewall	Existing Clause : Reports on risk analysis of firewall rules based on bank’s own current Risk Matrix which will learn and develop on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc.	Modified Clause: Reports on Best practice assessment of firewall rules based on OEMs Risk Matrix as well as industry standards such as CIS checks which will learn and about rules on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc. Justification: Every OEM has their own analytics engine/dashboard metrics. Our platform can provide detailed information around Best practice assesment and feature adoption for rules in the deployed enviroment. It also perform checks against industry standards such CIS.This ensures that the security rules are configured in the best way possible.	It is clarified that OEM's risk matrix customizable to bank's risk matrix is accepted.
194	58	External Firewall	External Firewall	Existing Clause : Reports on risk analysis of firewall rules based on bank’s own current Risk Matrix which will learn and develop on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc.	Modified Clause: Reports on Best practice assessment of firewall rules based on OEMs Risk Matrix as well as industry standards such as CIS checks which will learn and about rules on an ongoing basis and would be based on Zone to Zone, Subnet to Subnet or IP to IP etc. Justification: Every OEM has their own analytics engine/dashboard metrics. Our platform can provide detailed information around Best practice assesment and feature adoption for rules in the deployed enviroment. It also perform checks against industry standards such CIS.This ensures that the security rules are configured in the best way possible.	It is clarified that OEM's risk matrix customizable to bank's risk matrix is accepted.
195	59	External Firewall	137	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic	Requested Clarification on SSL inspection policy differentiation : Kindly request the department to provide more clarity on what you are trying to achieve.Are you looking to differentiate traffic, such as banking and finance, to ensure that you do not decrypt it for compliance, business, and regulatory purposes?	It is clarified that the NGFW should have the option of applying decryption policy for selected traffic.

196	59	External Firewall	137	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic	Requested Clarification on SSL inspection policy differentiation : Kindly request the department to provide more clarity on what you are trying to achieve.Are you looking to differentiate traffic, such as banking and finance, to ensure that you do not decrypt it for compliance, business, and regulatory purposes?	It is clarified that the NGFW should have the option of applying decryption policy for selected traffic.
197	59	External Firewall	137	The NGFW shall support the ability to have a SSL inspection policy differentiate between personal SSL connections i.e. banking, shopping, health and non-personal traffic	Requested Clarification on SSL inspection policy differentiation : Kindly request the department to provide more clarity on what you are trying to achieve.Are you looking to differentiate traffic, such as banking and finance, to ensure that you do not decrypt it for compliance, business, and regulatory purposes?	It is clarified that the NGFW should have the option of applying decryption policy for selected traffic.
198	60	SIEM	60	The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank.	Please confirm, the ask is store 3 months online data and 1 year archived data, these archived logs must be retrievable for analysis by SIEM	It is clarified that your understanding is right
199	60	SIEM	60	The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank.	Please confirm, the ask is store 3 months online data and 1 year archived data, these archived logs must be retrievable for analysis by SIEM	It is clarified that your understanding is right
200	61	SIEM	9	The proposed solution should be sized for 5,000 sustained EPS at correlation layer initially per Data centre but should be able to handle peak >License deployed EPS (additional 5000 EPS to take care of spikes/ burst / outbreak / flood in traffic) at correlation layer without dropping events or queuing events (for SIEM) per Data Centre.	Does it mean overall Bank required 10K EPS. 5K EPS for DC and DR each? Is any peak EPS determined or calculated or any observation around it. Please clarify	Please refer to the amendment
201	61	SIEM	18	The solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs	Q: Please specify agentless collection of logs are from which devices? E.g. windows, db etc..	It is clarified that the required details should be obtained from OEMs
202	62	SIEM	25	The solution should be able to integrate with incident management and leading ticketing tools like SMAX, Manage engine etc	Q: Please specify the ticketing tool and whether it support API integration.	It is clarified that the information will be given to successful bidder.
203	64	SIEM	53	The solution should provide automated cyber threat intelligence from internal, open source and subscribed threat intelligence feeds including but not limited to STIX/TAXI, openIOC etc. formats. The correlations engine should be updated with real time security intelligence updates from the OEM.	Please clarify whether TNGB is looking for a 3rd party threat intel feed along with out of the box threat intel feed provided by the SIEM vendor?	It is clarified that Proposed SIEM should support integration of third party threat intel feed arranged by the bank.

204	64	SIEM	53	Bidder will provide & integrate subscribed leading/popular Threat Intelligence tools like community edition of Virus Total or similar for IOCs feeds as a part of the proposed SIEM solution for alert triage.	Please clarify whether TNGB is looking for a 3rd party threat intel feed along with out of the box threat intel feed provided by the SIEM vendor?	It is clarified that threat intel feed provided by OEM of SIEM along with SIEM by default should be available to the bank.
205	65	SIEM	56	"The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier."	The technical specification mentioned here is favourable to a specific OEM. Having technical requirements specific to a single OEM will result in unfair advantage and limits the participation of other OEM's who are technically qualified, Which is not in line with our Honorable Government's Make in India / AtmaNirbhaar Bharat policy. Kindly requesting to remove this clause.	Please refer to the amendment
206	65	SIEM	56	"The solution must display traffic profiles in terms of packet rate/ traffic volume/ protocol. This capability must be available for complete TCP sessions analysis e.g. application traffic, session recreation and visualization. For example, throw alert if any services within the organization is using an unknown protocol to a foreign IP address with which there was never any communication done earlier."	The technical specification mentioned here is favourable to a specific OEM. Having technical requirements specific to a single OEM will result in unfair advantage and limits the participation of other OEM's who are technically qualified, Which is not in line with our Honorable Government's Make in India / AtmaNirbhaar Bharat policy. Kindly requesting to remove this clause.	Please refer to the amendment
207	65	SIEM	58	SIEM Deployment requirement is Active in DC & passive in DR.	Please clarify whether TNGB is looking for DC Active with HA setup and DR Passive with HA setup or it will be DC Active with standalone setup and DR Passive with standalone setup.	It is clarified that collection should happen at both the sites and analysis should happen at active site.
208	65	SIEM	58	SIEM Deployment requirement is Active in DC & passive in DR.	Q: Please elaborate on passive in DR, only the collection has to be happened in DR and actively DC will be managed?	It is clarified that collection should happen at both the sites and analysis should happen at active site.
209	65	SIEM	58	SIEM Deployment requirement is Active in DC & passive in DR.	Kindly clarify whether the SIEM Solution mentioned should be in High Availability or Not.	It is clarified that collection should happen at both the sites and analysis should happen at active site.

210	65	SIEM	60	The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank.	Please clarify whether the logs will be sent to SIEM platform from an existing Syslog server or bidder needs to integrate all the data sources directly with SIEM and collect logs.	It is clarified that the successful bidder should integrate all the data sources directly with SIEM and collect logs
211	65	SIEM	68	The solution shall allow bandwidth management, rate limiting, at the log collector level	Q: It contradicts with the near real time correlation, if we limit the bandwidth the purpose of having real time logs and correlation would get defeated. Please consider to remove the point.	Please adhere to the terms and conditions
212	66	SIEM	76	The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities	The alerts triggered by SIEM is handelled and managed at ITSM tool, so list of pending items is outside the scope of SIEM, hence requesting to remove the point	It is clarified that the SIEM should have provision to track the status of alerts raised by it.
213	66	SIEM	80	"SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.)"	"Ability to Perform Deep packet inspection" in SIEM solution is a specification favaourable to one specific OEM. Having technical requirements specific to a single OEM will result in unfair advantage and limits the participation of other OEM's who are technically qualified. The technical specification mentioned here is favourable to a specific OEM, which is not in line with our Honorable Government's Make in India / AtmaNirbhaar Bharat policy. Kindly requesting to remove this clause.	Please refer to the amendment
214	66	SIEM	80	"SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.)"	"Ability to Perform Deep packet inspection" in SIEM solution is a specification favaourable to one specific OEM. Having technical requirements specific to a single OEM will result in unfair advantage and limits the participation of other OEM's who are technically qualified. The technical specification mentioned here is favourable to a specific OEM, which is not in line with our Honorable Government's Make in India / AtmaNirbhaar Bharat policy. Kindly requesting to remove this clause.	Please refer to the amendment
215	66	SIEM	80	SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.)	Q: Please clarify deep packet inspection are part of NBAD L-7 flow inspection.	It is clarified that the solution should have ability to perform DPI in layer 4 as well as layer 7 flow inspection

216	66	SIEM	80	SIEM should have ability/provision to perform Deep packet inspection using NTA/NBAD along with Layer-4 ,Layer-7 flow inspection. (Bidder does not require to provide NTA and NBAD in this bid.)	Deep Packet Inspection is very important and effective way to get more visibility of the security posture of an organization. Requesting TNGB to include the DPI with minimum 250 mbps throughput to the the existing scope. SIEM and DPI solutions should be from the same OEM and solution should allow manage, monitor and investigation of logs and packets data from a single console and correlate logs and packets using same rule.	It is clarified that the solution should have ability to perform DPI in layer 4 as well as layer 7 flow inspection
217	66	SIEM	83	Solution should monitor all changes: Where the change was made, who made the change, when the change was made, what change was made, and whether or not the change was authorized -all through a defined control process, enabling verification and audit. Solution should provide real-time alerts on unauthorized changes, enabling the fastest response so you can investigate why the change process was circumvented.	Is this referred for the changes made on SIEM, also change management is a different process handeled outside the scope of SIEM, requesting to remove the point	Please adhere with the specifications in the RFP.
218	66	SIEM	83	Solution should monitor all changes: Where the change was made, whomade the change, when the change was made, what change was made,and whether or not the change was authorized -all through a definedcontrol process, enabling verification and audit.Solution should provide real-time alerts on unauthorized changes,enabling the fastest response so you can investigate why the changeprocess was circumvented.	Is this referred for the changes made on SIEM, also change management is a different process handeled outside the scope of SIEM, requesting to remove the point	Please adhere with the specifications in the RFP.
219	67	WAF	1	The WAF Appliance must be a dedicated hardware and it should not be clubbed with Load Balancers/ADC.	The WAF Appliance must be a dedicated hardware. Justification : A holistic solutuion should cover http and non-http load balancing as well.	Please refer to the amendment
220	67	WAF	1	The WAF Appliance must be a dedicated hardware and it should not be clubbed with Load Balancers/ADC.	Requesting the Bank to change this clause as: The WAF Appliance must be a dedicated hardware.	Please refer to the amendment
221	67	WAF	1	The WAF Appliance must be a dedicated hardware and it should not be clubbed with Load Balancers/ADC.	Request bank to chang this to "**The WAF Appliance must be a dedicated hardware**." As a holistic solutuion should cover http and non-http load balancing as well.	Please refer to the amendment
222	67	WAF	4	Proposed appliance should have minimum 2 X 10G Fibre, and 4x1 G Fibre ports provisioned	Requesting the Bank to kindly confirm if is it 4X1G copper or 4X1G Fiber, because already 2X10G has been asked in the RFP	Please refer to the amendment

				from the start. There should be separate out of band management port as well	and required throughput is only 1 Gbps. So what is the use of 1G Fiber port, kindly clarify.	
223	67	WAF	4	Proposed appliance should have minimum 2 X 10G Fibre, and 4x1 G Fibre ports provisioned from the start. There should be separate out of band management port as well	Requesting the Bank to kindly confirm if is it 4X1G copper or 4X1G Fiber, because already 2X10G has been asked in the RFP and required throughput is only 1 Gbps. So what is the use of 1G Fiber port, kindly clarify.	Please refer to the amendment
224	67	WAF	7	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure.	The solution must have inbuilt fail-over functionality in case of hardware failure. Justification: WAF is a critical component in a banking environment and hence we should ensure that all traffic are inspected by WAF.It is deployed in HA to ensure that there is no security breach happens because of bypassing WAF.	Please refer to the amendment
225	67	WAF	7	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure.	Requesting the Bank to change this clause as: The solution must have inbuilt fail-over functionality in case of hardware failure.	Please refer to the amendment
226	67	WAF	7	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure.	Request bank to change this to "**The solution must have inbuilt fail-over functionality in case of hardware failure**." as WAF is a critical component in a banking environment and hence we should ensure that all traffic are inspected by WAF.It is deployed in HA to ensure that there is no security breach happens because of bypassing WAF.	Please refer to the amendment
227	67	WAF	7	The solution must have inbuilt bypass segments to ensure that fail open in case of hardware failure.	Request you to remove this clause:- In the clause no 72, bank has requested devices in HA (Active-Active & Active Passive) considering that point we are requesting you to remove this clause.	Please refer to the amendment
228	67	SIEM	77	The solution should allow users to initiate and track alert related mitigation action items. The portal should allow reports to be generated on pending mitigation activities	The alerts triggered by SIEM is handelled and managed at ITSM tool, so list of pending items is outside the scope of SIEM, hence requesting to remove the point	It is clarified that the SIEM should have provision to track the status of alerts raised by it.
229	68	WAF	13-d	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.	Request you to amend the clause:- WAF works on the application layer and policy applies per application/host wise. According to this clause if we apply policy different for different pages of application then it will contradict the policy state and it will affect the overall security. We request you to amend the clause: -The solution must support the configuration to allow some applications to be in detection / learning mode without impacting other host/applications which can be in block mode.	Please refer to the amendment
230	68	WAF	13-d	The solution must support the configuration to allow some pages in a web application to be in blocking mode and some pages to be in detection / learning mode.	Requesting Bank to amend the clause as: The solution must support the configuration to allow some applications to be in detection / learning mode without impacting other host/applications which can be in block mode.	Please refer to the amendment

231	69	WAF	15	The Proposed WAF Solution Should support ICAP, API or other supporting integration with different security devices for file scanning, sandboxing requests etc (industry leading security solutions)	Integration with ICAP and API not supported. Only Fireeye is supported.	Please adhere to the specification of the RFP
232	69	WAF	15-b	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	This feature is supported with additional solution - ABP. For plain WAF gw, this needs to be removed	Please refer to the amendment
233	69	WAF	15-b	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	OEM Specific Clause, Request you to please remove this clause. Proposed solution has a capability to mitigate Brute Force Attack in the device itself, which every WAF OEM does as a part of OWASP TOP 10.	Please refer to the amendment
234	69	WAF	15-b	Proposed solution should have capability to redirect Brute force attack traffic to Honey Pot page.	Requesting Bank to remove this clause. Proposed solution has a capability to mitigate Brute Force Attack in the device itself, which every WAF OEM does as part of OWASP TOP 10.	Please refer to the amendment
235	71	WAF	42	The proposed Solution should remove application error messages from pages sent to users	Clarification Required. We understand that the Bank is looking to throw a customized page in case of any error message coming from the server side. Please confirm.	It is clarified that your understanding is right
236	71	WAF	42	The proposed Solution should remove application error messages from pages sent to users	Clarification Required. We understand that the Bank is looking to throw a customized page in case of any error message coming from the server side. Please confirm.	It is clarified that your understanding is right
237	71	WAF	50	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	Clarification Required:- We would like to understand how many application bank is looking to onboard on WAF for API security from and how many apps are currently running on API basis.	It is clarified that the details will be provided to successful bidder.
238	71	WAF	50	Solution should support reverse engineering for API Schema via Learning mode, should able to Discover New API Paths/ Shadow paths/ Stale API Paths/ Authenticated Paths/ Unauthenticated Paths.	Clarification Required:- We would like to understand how many application bank is looking to onboard on WAF for API security from and how many apps are currently running on API basis.	It is clarified that the details will be provided to successful bidder.
239	73	WAF	73	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	Request bank to change this to "**The solution must have inbuilt fail-over functionality in case of hardware failure**." as WAF is a critical component in a banking environment and hence we should ensure that all traffic are inspected by WAF.It is deployed in HA to ensure that there is no security breach happens because of bypassing WAF.	Please refer to the amendment
240	73	WAF	77	The Solution should also have a runtime plugin that would get installed on the Application Servers and protect applications at runtime specially from Zero Day Attacks.	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	Please refer to the amendment

241	73	WAF	77	The Solution should also have a runtime plugin that would get installed on the Application Servers and protect applications at runtime specially from Zero Day Attacks.	Request bank to change this as "**The Solution should protect applications at runtime specially from Zero Day Attacks."** Each OEM have a different approach to protect zero day attack and hence requesting you to ammend the changes for larger participation.	Please refer to the amendment
242	73	WAF	77	The Solution should also have a runtime plugin that would get installed on the Application Servers and protect applications at runtime specially from Zero Day Attacks.	Requesting the Bank to change this clause as: The Solution should protect applications at runtime specially from Zero Day Attacks.	Please refer to the amendment
243	73	WAF	77	The Solution should also have a runtime plugin that would get installed on the Application Servers and protect applications at runtime specially from Zero Day Attacks.	We understand bank is looking for zero day attack protecion from automatic signature protection.	Please refer to the amendment
244	73	WAF	78	The solution should build a profile of the runtime environment and accordingly only allow trusted requests.	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.
245	73	WAF	79	The runtime protection should not rely on any signatures	We understand that the Bank is looking for automatic signature protection in case of zero day attack. Please confirm.	It is clarified that the bank is looking for automatic protection in case of zero day attack.
246	73	WAF	79	The runtime protection should not rely on any signatures	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	It is clarified that the bank is looking for automatic protection in case of zero day attack.
247	73	WAF	79	The runtime protection should not rely on any signatures	We understand bank is looking automatic signature protection in case of zero day attack. Please confirm	It is clarified that the bank is looking for automatic protection in case of zero day attack.
248	73	WAF	80	The runtime protection must not connect to Internet for any updates.	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the

						solution offered to the bank.
249	73	WAF	81	The runtime protection should protect against attacks like path traversal, CSRF, SQL Injection etc.	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.
250	73	WAF	82	The runtime protection must also identify weak ciphers being used in the Application.	This feature is supported with additional solution - RASP. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.
251	73	WAF	83	The solution should be configurable to block the IOCs	we understand this clause talks about the scoring parameters of the threat basis which attakcs will be blocked and signautres will be created. Please confirm	It is clarified that the IOCs received from threat intelligence agencies should be configured in WAF to block.
252	73	WAF	83	The solution should be configurable to block the IOCs	we understand this clause talks about the scoring parameters of the threat basis which attakcs will be blocked and signautres will be created. Please confirm	It is clarified that the IOCs received from threat intelligence agencies should be configured in WAF to block.
253	74	WAF	74	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	As the device asked is in HA as per point No.51, 72 of having the bypass cards on the WAF Appliance. During hardware failure the traffic will continue to flow through WAF appliance without any mitigation and Security checks enforced during the time of an attack.However, WAF is a layer7 solution which is placed nearest to application and inspects HTTP/S protocol over L3 & L4 information, WAF will typically operates at the data link layer and will lack the ability to inspect and make decisions based on higher-layer information, such as IP addresses, ports, or content. Request you to remove this clause.	Please refer to the amendment

254	74	WAF	84	The solution should address and mitigate the OWASP Top 10 web application/ mobile application security vulnerabilities. The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the OWASP Application Security Top 10 and also provide suggestions/shortcuts to address the compliances and configure policies for it.	Vendor specific point. Imperva mitigates all OWASP Top10 attacks, however there is no separate OWASP compliance dashboard	It is clarified that if the OEM is not having inbuilt dashboard for OWASP compliance, the dash board should be customised for the bank to include OWASP compliance status.
255	74	WAF	85	Solution should support API security including support for uploading swagger file.	This feature is supported with additional solution - API Security. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.
256	74	WAF	87	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behaviour analysis.	This feature is supported with addiotional solutions such as ABP. For plain WAF gw, remove heuristics behaviour.	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.
257	74	WAF	87	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behaviour analysis.	Clarification Required. For Bot sizing kindly let us know the no of request per second/ month / year to factor the Bot along with WAF	It is clarified that the details will be provided to successful bidder.
258	74	WAF	87	It should provide advanced BOT detection mechanism based on smart combination of signature-based and heuristic behaviour analysis.	Clarification Required. For Bot sizing kindly let us know the no of request per second/ month / year to factor the Bot along with WAF	It is clarified that the details will be provided to successful bidder.
259	74	WAF	88	The Proposed WAF Solution should provide built-in L7 layer DDoS detection and mitigation features based on machine learning and behavioural analytics and dynamic signatures. It should have CAPTCHA support or other mechanism to avoid distributed attack. Solution should support Behavioural L7 DDoS mitigation to detect attacks without human	This feature is supported with additional solution - ABP. For plain WAF gw, this needs to be removed	It is clarified that additional solutions required to meet the specification requirements of WAF should be included in the solution offered to the bank.

				intervention.		
260	74	WAF	89	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Vendor specific point. Imperva mitigates all application related attacks. However this is a client side functionality.	It is clarified that the WAF should impose the requirements on client side to ensure the data transmission between the client and server is secured.
261	74	WAF	89	The Proposed WAF solution must provide capabilities to obfuscate sensitive field names to defeat Man-in-The-Browser Attacks	Request you to remove the clause:- This clause is specific to vendor and provides an undue advantage	It is clarified that the WAF should impose the requirements on client side to ensure the data transmission between the client and server is secured.
262	74	WAF	90	Should provide encryption for user input fields to protect from browser based malwares stealing users credentials. Able to defend against browser based keyloggers that attempt to capture user's keystrokes and steal user credential using Field Encryption	Vendor specific point. Imperva mitigates all application related attacks. However this is a client side functionality.	It is clarified that the WAF should impose the requirements on client side to ensure the data transmission between the client and server is secured.
263	74	WAF	90	Should provide encryption for user input fields to protect from browser based malwares stealing users credentials. Able to defend against browser based keyloggers that attempt to capture user's keystrokes and steal user credential using Field Encryption	Request you to remove the clause:- This clause is specific to vendor and provides an undue advantage	It is clarified that the WAF should impose the requirements on client side to ensure the data transmission between the client and server is secured.
264	74	WAF	92	Proposed solution should be able to track unused elements in the policy and suggest to remove them after a specified period of time	Vendor specific point. Imperva does not recommend removal/modification of any security policy. The polciies do not affect the performance of WAF	Please adhere to the specification of the RFP
265	74	WAF	93	Proposed Solution should have ability to automatically detect software/Server technology used on backend side to define	As per the clause, we understand that bank is looking for Server side request forgery kind of attacks that eventually protects the server from getting compromised. Please clarify?	It is clarified that the solution should configure rules based on the

				signature sets required for defined Proposed Solution policy.		underlying server OS, web server
266	74	WAF	93	Proposed Solution should have ability to automatically detect software/Server technology used on backend side to define signature sets required for defined Proposed Solution policy.	As per the clause, we understand that bank is looking for Server side request forgery kind of attacks that eventually protects the server from getting compromised. Please clarify?	It is clarified that the solution should configure rules based on the underlying server OS, web server
267	74	WAF	96	Server Load Balancing for non-http application also then include the following point	Vendor specific point. Contradicts point 1	Please refer to the amendment
268	74	WAF	96	Server Load Balancing for non-http application also then include the following point	Request bank to kindly remove this point as this is typo.	Please refer to the amendment
269	74	WAF	97	The solution should include both HTTP and Non-HTTP load balancing. It should support all common load balancing method with priority-based group activation.	Vendor specific point. Contradicts point 1	Please refer to the amendment
270	75	WAF	75	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	As the device asked is in HA as per point No.51, 72 of having the bypass cards on the WAF Appliance. During hardware failure the traffic will continue to flow through WAF appliance without any mitigation and Security checks enforced during the time of an attack.However, WAF is a layer7 solution which is placed nearest to application and inspects HTTP/S protocol over L3 & L4 information, WAF will typically operates at the data link layer and will lack the ability to inspect and make decisions based on higher-layer information, such as IP addresses, ports, or content. Request you to remove this clause.	Please refer to the amendment
271	76	Web Proxy with DLP	10	The solution should have Global web content monitoring services to provide regular and updated caching algorithms and signatures on regular intervals to the on-premises WSS to enable effective caching for popular web 2.0 and video sites. The solution should support granular web 2.0 application control over web eg. Facebook controls like block file upload, block posting text, blocking specific version of Internet Explorer, etc. This blocking should be based on signature and not URL. The application signature database should be updated periodically by the vendor (from their cloud).	Forcepoint advise to remove this pointer or modify the clause to have caching feature to be removed as its not effectivly protect todays Dynamic web content	Please adhere to the specifications of RFP.

272	76	Web Proxy with DLP	13	Also the solution must have the option to allow or deny a particular domain or destination for a user or IP group for a permanently or for a specific time period. Solution should be able to block domains which are containing alpha numeric andspecial characters.	Forcepoint request to modify the spec as "the solution must have a user or IP group for a permanently or for a specific time period. containing alpha numeric andspecial characters.	Please refer to the amendment.
273	76	Web Proxy with DLP	15	The solution should support following actions for websites/Applications like allow, monitor, block, time-based access.	Request to modify the spec to support following actions for web s Monitor / confirm.	Please adhere to the specifications of RFP.
274	76	WAF	76	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	Request you to remove this clause:- In the clause no 72 & 93 bank has requested devices in HA (Active-Active & Active Passive) considering that point we are requesting you to remove this clause.	Please refer to the amendment
275	77	WAF	77	In layer 2 deployment, the WAF must have an internal bypass segment that can be used incase of Hardware failure of WAF.	The solution must have inbuilt fail-over functionality in case of hardware failure.	Please refer to the amendment
276	79	Web Proxy with DLP	54	Solution should be able to restrict Users to download certain files based on file types, size, extensions etc. Also the solution should be capable of blocking specific set of files downloads for specific user groups. Even if the file types are blocked globally,exception based on URLs, IPs, domains should be allowed.	Download can be restrcited based on file size, Request to modify the spec as "Solution should be able to restrict Users to download certain files based on file types, extensions etc. Also the solution should be capable of blocking specific set of files downloads for specific user groups. Even if the file types are blocked globally,exception based on URLs, IPs, domains should be allowed."	Please refer to the amendment.
277	81	Web Proxy with DLP	94	solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access user.	Forcepoint request to modify the Spec as follows "The Solution shall support role-based administration such as Administrator, Auditor, Incident Manager, Database Reader, and Read- only access user."	Please refer to the amendment.
278	81	Web Proxy with DLP	98	solution should support a web interface that includes a tool that traces & can simulate client requests as if they were made by the end users. It should describe how Web Proxy processes the request and can be used for troubleshooting purpose. It should also support policy simulating functionality.	Forcepoint request to remove the spec as the same is not viable achieved with Proxy solution.	Please refer to the amendment.
279	83	Web Proxy with DLP	120	The centralized management should be provided without the support of additional hardware/server (preferably) and if any additional devices required for the management of solution, it should be mentioned clearly.	Forcepoint Proxy required separate Management server	Please refer to the amendment

280	85	CLMS	2.1	The log data needs to be stored in an archive for forensic analysis and regulatory compliance requirements.	Please confirm the Archival retention period	It is clarified that The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank. The retention period is not related to EPS or size.
281	85	CLMS	2.3	The retention duration should be flexible (current requirement is 5 years for VPN logs and 1 year for other logs)	Please seggregate the retention based on size or EPS as well as based on Onoline searchable or Archiaval restoration. The current clause is not clear on storage retention	It is clarified that The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank. The retention period is not related to EPS or size.
282	85	CLMS	2.3	The retention duration should be flexible (current requirement is 5 years for VPN logs and 1 year for other logs)	Kindly specify Log Retention Period for Online & Offline Storage	It is clarified that The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank. The retention period is not related to EPS or size.
283	85	CLMS	2.6	The Solution should support the collection of logs from at least 1000 devices from day one and should be scalable to support a maximum of 2000 devices (data sources) during the contract period.	Whether 1000 devices are located in different locations? How many locations are present & How is the connectivity between these locations?	It is clarified that the devices are spread across 1000 locations and all are connected to central site.

284	85	CLMS	4.1	The CLMS should be on-premises with a clear separation of the collection engine and the logging engine. The collection engine should be available in DC and DRS in active-active or active- passive mode depending on the Bank's decision.	In addition to this, please also add "Solution should allow to be installed on Hypervisor (VMware/Hyper-V/Azure/AWS) Platform over any Hardware and be accessible via any supported Web-based Browser access"	It is clarified that Virtualised environment will be provided by the bank for CLMS.
285	85	CLMS	4.2	The Solution should offer Single Global View of all the log data received from devices deployed across sites/geographies	Request you to please change this to "The Solution should offer Single Global Web View of all the log data received from devices deployed across sites/geographies and the Web UI should support RSA key strength of minimum 4096 bits"	Please adhere to the specifications of RFP.
286	85	CLMS	4.5	The Solution should be able to handle up to 5,000 Sustained EPS. The proposed Solution should take into account upgrades of hardware, software, licenses as applicable over the contract period at no additional cost to the Bank. The Solution should be scalable up to 10,000 Sustained EPS during the contract period.	Please confirm if the Hardware for 10K EPS scalability needs to be provided at the Bid time or supplied at the time of scaling based on needs.	It is clarified that the hard ware will be provided by the bank.
287	85	CLMS	4.6	The Solution should support the collection of logs from at least 1000 devices from day one and should be scalable to support a maximum of 2000 devices (data sources) during the contract period.	Also, there is no mention of retention period for logs. Kindlmy provide the data for sizing retention and archival storage for online and offline data retention.	It is clarified that The solution should be capable to store 3 Months data online on storage device and able to archive one year data from Syslog server provided by the bank. The retention period is not related to EPS or size.
288	85	CLMS	4.8	The Solution receiver or log collection component must store the data locally if communication with centralized server is unavailable. The minimum holding period shall be of 72 hours.	Please confirm the number of such locations where data needs to be collected from and no of EPS t such locations to consider the required storage for persistent data collection in case of communication breaks with centralized server or network issues	It is clarified that the locations are two.
289	86	CLMS	4.11	The Solution should be capable of retrieving the logs for analysis, reporting, and forensic purposes.	This is repeated clause	Please refer to the amendment

290	86	CLMS	4.13	The Solution's log receiver/collector component should be able to work in high availability (HA) mode. The following are important points to be noted regarding the high-level LMS architecture: (a) The log collection engine shall be deployed in HA within each DC and DRS of the Bank (b) Ability to handle a situation that involves once DC being unavailable, all services should work from DRS in near real-time without loss of any data.	At any point of time, entire log collection should be done at centralized DC. For HA and data resilience bank intends to have Data replication between DC & DR site with near-realtime sync along-with HA at log collector level only. Is this understanding correct . That means all event sources would send data to central site at one of DC at any given point of time, but the data collection traffic management needs to be done at Collector layer.	It is clarified that the understanding is correct. The loss of data due to lag in communication between DC and DR is accepted
291	86	CLMS	4.14	The Solution should be licensed based on the EPS count (and not licensed by the number of users, device types, and/or the number of network or end systems devices that are subject to logging).	Request you to please change this to "The Solution should be licensed based on the EPS count or the number of devices" This can help you to reduce the overall Total Cost of Ownership (TCO).	Please refer to the amendment
292	86	CLMS	4.14	The Solution should be licensed based on the EPS count (and not licensed by the number of users, device types, and/or the number of network or end systems devices that are subject to logging).	Please relax this clause as most log management solutions are based on size of data. If you could amend the clause for either size of data and /or EPS. Request to amend the clause as below… "The Solution should be licensed based on the EPS count or Size of data to be processed for the retention period (and not licensed by the number of users, device types, and/or the number of network or end systems devices that are subject to logging)."	Please refer to the amendment
293	86	CLMS	4.16	The Solution shall be integrated with the Bank's SIEM solutions so that logs may be forwarded to SIEM	What is the SIEM solution referred here?	It is clarified that the SIEM solution proposed by the bidder is referred here
294	86	CLMS	5.1	The Solution should provide a data aggregation technique to summarize and reduce the number of events stored in the master database.	Does Bank intend to store raw data entirely for retention period for compliance or want to reduce and filter the data with aggregations and ETL jobs?	It is clarified that the bank intends to store raw data entirely for the retention period. For viewing the data, the solution should be able to apply filters.
295	86	CLMS	5.6	The Solution architecture should be implemented in such a manner that there shall be no loss of data/logs during the execution of maintenance activities and	Q: Please provide relaxation on the point by modifying as near zero loss of data/logs	Please adhere to the terms and conditions of RFP

				failure of one or more Solution components and other similar reasons (like DR drills etc.)		
296	86	CLMS	5.7	The Solution must have a toolkit & /or interfaces to allow for creation /integration with unsupported legacy or custom event sources	This is repeated clause	Please adhere to the specifications of RFP.
297	87	DAM	1	DAM solution should treat if one database is having 5 different instances, then it will be considered as single database. Also, number of cores will not be counted for a particular database rather the same should be considered as single database.	Each vendor uses different mechanisms and attributes to consider the number of licenses. We consider the DAM licenses based on number of instances running in the server. Hence, we request to change the clause as below: “DAM solution should treat if one database is having 5 different instances, then it will be considered as single server or 5 instances of DAM licenses. Also, number of cores will not be counted for a particular database rather the same should be considered as based on number of database instances.”	Please adhere to the terms and conditions of the RFP
298	87	CLMS	5.16	The Solution shall be integrated with the Bank's SIEM solutions so that logs may be forwarded to SIEM	Please confirm which SIEM is being currently used by Bank	It is clarified that the SIEM solution proposed by the bidder is referred here
299	87	CLMS	5.6	The Solution must provide support for various methods that can be used to alert concerned officials about important and critical events (e.g., SMTP, SMS, etc.). The Gateway will be provided by the bank.	Is there any specific custom integration with existing landscape of applications which needs to to be factored in proposal.	It is clarified that no custom integration available as on date.
300	87	CLMS	5.8	The Solution should support the forwarding of raw logs to multiple destinations at the same time.	What is the epxectation from this setup requirement? IN a cenralized CLMS all data would need to be setup to be forwarded to one location at a time. If this is a requirement, please clarify the use case so that we can consider the solution accordingly	It is clarified that CLMS should be able to send the logs to SIEM, and other backup logging devices at the same time
301	87	CLMS	6.3	The Solution must provide fully customizable queries and report libraries to define reports	Please change this to "The Solution must provide fully customizable queries and report libraries to define reports and the custom reports should not need additional licenses"	Please adhere to the terms and conditions of the RFP
302	87	CLMS	7.2	The Solution should provide flexibility to the Administrator for controlling the replication and should also perform incremental synchronization between components of the Solution deployed across different locations.	Please clarify that the Replication means data replication between DC and DR that needs to be factored within the solution itself with no 3rd party tool dependency.	It is clarified that the replication between sites should be factored within the solution.

303	88	DAM	3	Creation of an inventory through auto discovery of all structured/unstructured databases and database users, deployed across the enterprise.	For more no of RFP participation, We request to change the specification as below: "Creation of an inventory through auto discovery of all databases and database users, deployed across the enterprise."	Please adhere to the specifications of RFP.
304	88	DAM	4	The proposed DAM solution should be able to monitor in scope structured/unstructured database without dropping any log.	For more no of RFP participation, We request to change the specification as below: "The proposed DAM solution should be able to monitor database without dropping any log.	Please adhere to the specifications of RFP.
305	88	DAM	10	The solution should be able to monitor and detect breaches/anomalies for all the structured/unstructured (NoSql) databases like MSSQL, MYSQL, PostgreS, Oracle, mongo DB etc. including Big data databases(size more than 10 TB).	Requesting the Bank to provide the breakup of databases in terms of type, version, location & number of cores for each database.	It is clarified that the details will be provided to successful bidder.
306	88	DAM	10	The solution should be able to monitor and detect breaches/anomalies for all the structured/unstructured (NoSql) databases like MSSQL, MYSQL, PostgreS, Oracle, mongo DB etc. including Big data databases(size more than 10 TB).	The term big data refers to large data sets, usually measured in terabytes or petabytes, that are analyzed to provide business insights. As seen in banking industry banks are not usually using these big data and often these are cloud based. Is bank using any big data databases in the environment. If no, We request to change the specification as below: "The solution should be able to monitor and detect breaches/anomalies for all the databases like MSSQL, MYSQL, PostgreS, Oracle, mongo DB etc."	Please adhere to the specifications of RFP.
307	88	DAM	10	The solution should be able to monitor and detect breaches/anomalies for all the structured/unstructured (NoSql) databases like MSSQL, MYSQL, PostgreS, Oracle, mongo DB etc. including Big data databases(size more than 10 TB).	We need to have breakup of databases in terms of type, version, location & number of cores for each database.	It is clarified that the details will be provided to successful bidder.
308	88	DAM	12	The solution should audit all types of database access across the organization regardless of database type or operating system of the host without relying on native auditing.	For OS that are not supported by agents, native auditing may be required for monitoring. Please confirm.	It is clarified that for OS which are not supporting agents, native auditing is accepted.
309	89	DAM	18	Minimum usage of system resources: For agent-based system, CPU utilization on the DB server should not exceed 3% beyond present utilization, however, the same should be configurable. For network monitoring the impact on monitored servers should be zero. At the same time, the solution should not overload the network and delay real time monitoring and attack mitigation measures. The solution should provide capping capabilities for CPU,	Restriction to 3%. Capping capability. This is OEM specific.	Please adhere to the specifications of RFP.

				RAM and disk on the agent based solution.		
310	89	DAM	18	Minimum usage of system resources: For agent-based system, CPU utilization on the DB server should not exceed 3% beyond present utilization, however, the same should be configurable. For network monitoring the impact on monitored servers should be zero. At the same time, the solution should not overload the network and delay real time monitoring and attack mitigation measures. The solution should provide capping capabilities for CPU, RAM and disk on the agent based solution.	CPU utilization on the DB server depends on the number of transactions cased at any given point of time. However, our solution consumes minimal CPU on the database server. As this 3% SLA would restrict other competitors who offers better technology on the activity monitoring. For more no of RFP participation, We request to change the specification as below: “Minimum usage of system resources: For agent-based system, CPU utilization on the DB server should be minimal. For network monitoring the impact on monitored servers should be zero. At the same time, the solution should not overload the network and delay real time monitoring and attack mitigation measures. The solution should provide capping capabilities for CPU, RAM and disk on the agent based solution.”	Please adhere to the specifications of RFP.
311	89	DAM	20	The solution should be able to integrate with external ticketing management tools (e.g. SMAX) for managing change.	As per best practices it is recommended to integrate the ticketing tool with the SIEM solution as organization collect all the security logs and performs the next level of incident management and ticketing. However integration should be supported from the ticketing tool as well. Hence, we request to relax this specification.	Please adhere to the specifications of RFP.
312	90	DAM	27	The solution should be capable of identifying the missing patches and report the same and should have capabilities of virtual patching of known vulnerabilities till the patch is installed.	This is OEM specific point. To be removed.	Please adhere to the specification of the RFP
313	90	DAM	29	The solution should provide optimum utilization of resources by using Load balancing between its devices, if it is using multiple boxes/gateways The solution should send all audit logs to centralised log management server.	Each vendor uses different monitoring and deployment options to monitor the activities of the databases. We use agent-based method to monitor the activity of the users on the database. We request bank to change the specification as below: “The solution should provide optimum utilization of resources on the database monitoring. The solution should send all audit logs to centralised log management server.”	Please refer to the amendment
314	92	DAM	64	The agent should not require a reboot of OS and DB after installation / configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. The solution should not use any 3rd Party software/support for any purpose	Requesting the Bank to amend this clause as: "Except AIX. AIX OS needs reboot to load DAM drivers once at the time of agent installation."	It is clarified that in case of AIX, reboot is accepted

315	92	DAM	64	The agent should not require a reboot of OS and DB after installation / configuration. Only one agent to be installed, no third-party agents permitted. All agents regardless of deployment mode should be managed from the centralized management console. The solution should not use any 3rd Party software/support for any purpose	Requesting the Bank to amend this clause as: "Except AIX. AIX OS needs reboot to load DAM drivers once at the time of agent installation."	It is clarified that in case of AIX, reboot is accepted
316	93	DAM	68	The solution should be able to support/monitor all database activities in OS like AIX, UNIX, HP UNIX, Linux, Solaris, Windows and Databases like Oracle, MS- SQL, MySQL, Postgres, Mongo at a minimum provided that DB vendors still support the versions in scope.	HP UNIX is supported without agents. Requesting acknowledgement.	Please adhere to the specification of the RFP
317	93	DAM	68	The solution should be able to support/monitor all database activities in OS like AIX, UNIX, HP UNIX, Linux, Solaris, Windows and Databases like Oracle, MS- SQL, MySQL, Postgres, Mongo at a minimum provided that DB vendors still support the versions in scope.	HP UNIX is supported without agents.	Please adhere to the specification of the RFP
318	93	DAM	71	All the reports should be generated at least in minimum time (within 120 seconds).	The reporting is dependent on type of report i.e. it's content, number of columns selected. So, difficult to assess time taken to fetch report.	It is clarified that automated reports should be generated within 120 seconds.
319	93	DAM	71	All the reports should be generated at least in minimum time (within 120 seconds).	The reporting is dependent on type of the report i.e. its content, number of columns selected. So, it will be difficult to ascertain the time taken to generate each report. Requesting the Bank to consider the same.	It is clarified that automated reports should be generated within 120 seconds.
320	93	DAM	75	The solution support individual user access auditing for packaged applications like SAP, Peoplesoft etc.	Does bank use this application with its own databases? Kindly provide the clarification with an example.	It is clarified that the databases of SAP, which is inbuilt database should be supported.
321	94	DAM	90	The solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use case possible. For example, the Username placeholder looks like (${Alert.username})	The solution by default generates logs in the event of violation of created policies. So, we don't see any reason to create custom-logs hence request you to please delete this feature	Please adhere to the specifications of RFP.
322	94	DAM	91	The solution must support generation/ both predefined as well as easy option to customize reports as per Bank's requirements in tabular views, pdf, data analysis graphical views, Excel, CSV formats etc.	For more no of RFP participation, we request to change the specification as below: "The solution must support generation/ both predefined as well as easy option to customize reports as per Bank's requirements in tabular views, .doc, .pdf, .xml, or .xls formats."	Please adhere to the specifications of RFP.

323	94	DAM	97	Solution should provide monitoring of all on-prem, cloud databases including PaaS, IaaS via centralise management console.	Does bank use any databases in cloud on PaaS, IaaS? If bank doesn't have any usage on cloud, we request bank to relax this specification.	It is clarified that the bank is proposing to have on prem cloud.
324	94	DAM	99	The solution should establish critical database security visibility and should only send events to SIEM rather than the entire logs. The solution should reduce SIEM index/telemetry fees with compute and storage costs.	Reducing/normalizing of the data on the event is a SIEM capability. DAM solution can send the event to the SIEM solution where as SIEM solution can normalize the log based on relevant information. Hence, we request to change the clause as below: "The solution should establish critical database security visibility and should send relevant events to SIEM."	Please adhere to the specifications of RFP.
325	95	EDR	1.5	The proposed solution must support SNMP, Syslog, etc. for integration with all leading SIEM/SOC solutions. The Solution components must also be providing access over REST API's with OEM documentation.	We have API integration on cloud base management, with regards to on prem,we have On-prem REST APIs in on Roadmap for end of this year. Will a letter of commitment work?	Please adhere to the specifications of RFP.
326	95	EDR	1.7	The proposed Endpoint Detection & Response can be on-premise :	Can EDR server run from public cloud , Can EDR be a cloud based SaaS solution	It is clarified that the EDR solution should be on prem only.
327	95	EDR	1.8	The solution offered should be deployed at DC and DRS on-premise :	Can EDR server run from public cloud , Can EDR be a cloud based SaaS solution	It is clarified that the EDR solution should be on prem only.
328	96	EDR	2.2	The proposed solution must have no dependency on signature based solution with typical use cases covered as below -IOC Detection (Malware & Methodology TTP's), -Intelligence feed integration, -Custom IOC creation, -Sweeping for openIOC, -Triaging an alert, -Containment/Isolation of a threat/machine, -Tracking compromised user activity , -Command-line visibility, -Investigating lateral movement, -Data staging and exfiltration, -Suspected anti-forensics activity -Investigating suspected rootkits & backdoors -Data Acquisition - Live Forensics -Hunting exercise like Stacking data & finding the unknown threats based on endpoint and server activity anomalies.	For threating hunting the managmant should be on cloud request bank to modify the clause accrordinly	Please adhere to the specification of the RFP

329	96	EDR	2.2	The proposed solution must have no dependency on signature based solution with typical use cases covered as below-IOC Detection (Malware & Methodology TTP's),-Intelligence feed integration,-Custom IOC creation,-Sweeping for openIOC,-Triaging an alert,-Containment/Isolation of a threat/machine,-Tracking compromised user activity ,-Command-line visibility,-Investigating lateral movement,-Data staging and exfiltration,-Suspected anti-forensics activity-Investigating suspected rootkits & backdoors-Data Acquisition- Live Forensics-Hunting exercise like Stacking data & finding the unknown threats based onendpoint and server activity anomalies.	For threating hunting the managmant should be on cloud request bank to modify the clause accrordinly	Please adhere to the specification of the RFP
330	96	EDR	2.3	The proposed solution must support OS versions like Windows, Linux Versions like RHEL, Ubuntu, SUSE, Open SUSE, Oracle Linux	On-prem EDR doesn't support Linux Versions like RHEL, Cent OS, Ubuntu, SUSE, Open SUSE, Oracle Linux as we support this capability through our server security solution. Request bank to reconsider and allow us to propose server security solution for Linux for this capability apart from endpoint security solution for EDR	It is clarified that server security solution may be provided for servers. However, the end point based EDR solution and server based EDR solution should be of same make.
331	96	EDR	2.4	The proposed solution must be a software agent and must co-exist with any other existing Anti-virus or endpoint management solutions. There should be no dependency on the existing AV engine or other endpoint features for the proposed solution capability.	As per best practice, no two Anti-Virus / Anti-Malware engine should co-exist as they can cause collision of functionality. So please amend this clause as "except for Anti-Malware capabilities, solution should co-exist with other AVs"	It is clarified that the solutions which co exist with Windows Defender(existing AV solution) is expected to be quoted by the bidder. However if the EDR solution proposed by the bidder is not capable to co exist with Windows Defender AV, the solution with both AV and EDR of same make may be quoted without additional cost to the bank.

332	96	EDR	2.4	The proposed solution must be a software agent and must co-exist with any other existing Anti-virus or endpoint management solutions. There should be no dependency on the existing AV engine or other endpoint features for the proposed solution capability.	As per best practice, no two Anti-Virus / Anti-Malware engine should co-exist as they can cause collision of functionality. So please amend this clause as "except for Anti-Malware capabilities, solution should co-exist with other AVs"	It is clarified that the solutions which co exist with Windows Defender(existing AV solution) is expected to be quoted by the bidder. However if the EDR solution proposed by the bidder is not capable to co exist with Windows Defender AV, the solution with both AV and EDR of same make may be quoted without additional cost to the bank.
333	97	EDR	2.10 to 2.17	2.10 to 2.17	These points are related to Threat Hunting. For this to be available, please mention the solution can be hosted on cloud. With regards to Indian Data Laws, i.e data localization & hosted on MEITY empaneled CSP.	It is clarified that the solution proposed have to be deployed on prem only

334	98	EDR	2.12	Hunting and Search features across windows, MAC and Linux must be available at the minimum including key System parameters like Application Name, Browser (Name & Version), DNS Hostname, Driver Device Name, Driver Module (Address, in-tree, license, parameters, Signature, signer, status, return Trampoliner, signing hash alogorithm, signing Key, vermagic, version), Executable Exported (Dll & Function Name), Executable (Imported Function & Module Name), Executable Injected, Executable PE Type, Executable Resource Name, File Attributes, File Certificate Issuer, File Certificate Subject, File Download Mime Type, File Download Referrer, File Download Type, File Full Path, File MD5 Hash, File Name, File SHA1 Hash, File SHA256 Hash, File Signature Exists, File Signature Verified, File Stream Name, File Text Written, Group ID, Group name, HTTP Header, Host Set, IP Address, Local IP Address, Local Port, Login Failed, Login Record Type, Network Route FLags, Parent Process Name, Parent Process Path, Port Protocol & State, Process Arguments, Process Hidden, Process Name, Registry Key Full Path, Registry Key Value Name, Registry Key Value Text, Remote IP Address, Remote Port, Remote Login, Session length, shell command, shell type, socket protocol, Socket State, Socket Type, sudo command & its success, syslog event ID, Syslog event message, syslog file, syslog sender, syslog severity level, Service DLL, Service Mode, Service Name, Service Status, Service Type, Size in bytes, Task Flag, Task Name, Task reference, Task Status, Terminal Type, Timestamp - (Accessed, Changed, Created, Event, Last Login, Last Run, Modified, Started), URL, Username, Web Page Original URL, Web Page	On-premise EDR supports Windows for hunting and search features. For linux, Server Security's system security module allow incident response teams to take all of that historical telemetry metadata and query individual event logs in Server Security. Request bank to reconsider and allow us to propose server security solution for Linux for this capability	It is clarified that server security solution may be provided for servers. However, the end point based EDR solution and server based EDR solution should be of same make.

335	99	EDR	2.23	Security analysts during incident response activity must have the capability in the solution to remotely acquire or locally acquire individual or bulk at the least raw files, full disk, process memory, full memory, Power shell, Command shell history and driver memory images with supported metadata and file acquisitions using both API mode and/or RAW mode.	Requesting the Bank to exclude this functionalty from EDR Spec, as Bank can explore 3rd party solution like DFIR tools, which are better suggested for such data collection activites, as the collected data is huge in size.	Please adhere to the specifications of RFP.
336	99	EDR	2.23	Security analysts during incident response activity must have the capability in the solution to remotely acquire or locally acquire individual or bulk at the least raw files, full disk, process memory, full memory, Power shell, Command shell history and driver memory images with supported metadata and file acquisitions using both API mode and/or RAW mode.	Requesting the Bank to exclude this functionalty from EDR Spec, as Bank can explore 3rd party solution like DFIR tools, which are better suggested for such data collection activites, as the collected data is huge in size.	Please adhere to the specifications of RFP.
337	101	NTP Server	5	NTP System should have capability to synchronize the system time with multiple sources like NPL, NIC etc., or any other source subject to approval by bank	As per CERT Government Guidelines, all service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securly with time stamp data connect to the Network Time Protocol (NTP) Server. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC. Considering the above, this NTP being a real time device. Sertel GNSS Servers are stratum-1 time server which is directly linked (not over a network path) to a reliable source of UTC time such as GPS, Galileo, IRNSS, GNSS receiver communicating over satellites. We will install a GPS antenna at the respective DC & DR location for achieving this. We request you to please consider the same.	It is clarified that GPS Antenna with necessary accessories may be provided and configured to get the time from satellites

338	101	NTP Server	5	NTP System should have capability to synchronize the system time with multiple sources like NPL, NIC etc., or any other source subject to approval by bank	As per CERT Government Guidelines, all service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securly with time stamp data connect to the Network Time Protocol (NTP) Server. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC. Considering the above, this NTP being a real time device. Sertel GNSS Servers are stratum-1 time server which is directly linked (not over a network path) to a reliable source of UTC time such as GPS, Galileo, IRNSS, GNSS receiver communicating over satellites. We will install a GPS antenna at the respective DC & DR location for achieving this. We request you to please consider the same.	It is clarified that GPS Antenna with necessary accessories may be provided and configured to get the time from satellites
339	104	Asset and Patch Management	7	The inventory information should be stored along with date stamps & track changes like installation/ uninstallation, configuration changes, user/owner changes etc along with functionality of XML tagging. IT inventory should include all the details of hardware	Is Time stamp-based tracking acceptable?	It is clarified that the time stamp based tracking is acceptable.
340	104	Asset and Patch Management	9	Should provide details such as Quantity of licenses purchased and deployed in AIX, Windows and Linux Operating system.	How many Linux and AIX machines need to be monitored?	It is clarified that the details will be provided to successful bidder.
341	105	Asset and Patch Management	10	The solution should also have the capability to integrate with e-mailing System and short message services.	Will Bank provide the SMS gateway server through email. Since the solution needs detailed alerts will the Mobile app(Android and IOS0 based alerts be accepted?	It is clarified that the bank will provide SMS gateway and email gateway servers. Mobile app based alerts are not accepted now.
342	106	Asset and Patch Management	20	Software catalogue should allow for the entry of custom developed software titles & custom classification of standard applications based on user preferences.	Can we get some more information like which fields and information for custom software?	It is clarified that the custom developed software titles, classification and user are minimum fields required now.
343	106	Patch Management	21	Solution should check for entry of new end points into theBank's network and trigger alerts.	This feature is more related to a rogue device detection in the network. Please correct with use cases if the understanding is wrong	Please adhere to the specifications of RFP.
344	108	Patch Management	1	The System should be able to recognize files with hidden attributes that is in the following: 1. Hidden Files	Request bank to remove the hidden files attributes.	Please adhere to the specifications of RFP.

345	108	Patch Management	3	The solution should support local distribution points through preferred servers and endpoints and also peer downloading	Peer downloading between agents is not available. Please help us understand more about this requirement with use cases or kindly consider removing this caluse alone from the RFP	Please refer to the amendment
346	108	Patch Management	4	The Agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.	Can this be changed as The solution should have a fall back mechanism where the agent should connect with Central server if the assisgned distribution server is not available	Please refer to the amendment
347	108	Asset and Patch Management	7	The Solution should have ability to track standalone executable based applications on each computer i.e. Applications that do not need to be installed but just needs to execute a standalone program (Standalone applications/ executable/ portable programs needs to be tracked by the system)	Can the Tamil Nadu grama bank provide the list of portable "exe" to be identified from endpoints to achieve this action	It is clarified that the list of applications to be tracked will be provided to successful bidder.
348	108	Patch Management	7	The Solution should have ability to track standalone executable based applications on each computer i.e. Applications that do not need to be installed but just needs to execute a standalone program (Standalone applications/ executable/ portable programs needs to be tracked by the system)	Request bank to kindly remove this clause.	Please adhere to the specifications of RFP.
349	108	Asset and Patch Management	8	The solution should provide desktop admins capability to take remote control of endpoints for maintenance purposes. This feature should support copying files, removing files to/ from remote devices	Can additional agent be integrated to achieve this need? Like Quick assist, VNC, etc	It is clarified that no additional agents should be installed.
350	108	Patch Management	10	The solution should able to remove unauthorized, unlicensed software or any software installed in the endpoints and servers as required by Bank through the central management console	Patch Management - Please confirm if the end to end patch management is part of the bidders scope.	It is clarified that end to end patch management is part of bidders scope
351	108	Asset and Patch Management	44	The Solution should show trending and analysis of security configuration changes through advanced reporting.	Since we are discussing a patch management solution could you please help us with more details on which security changes need to be tracked	It is clarified that the changes made in the clients which affects the secured configuration requirements of the bank is expected to be reported by the solution.

352	110	Asset and Patch Management	25	The solution should support integration with other security solutions such as SIEM, Anti-Virus, IPS etc.	Integration with Antivirus is possible for software distribution, does default integration of defender will meet the objective and integration for SIEM and IPS using System and application is enough ?	It is clarified that the solution should co-exist with AV, IPS software installed in the endpoints and send the feed to SIEM through console on installation\uninstallation of software.
353	111	Asset and Patch Management	7	The solution should have auditing capabilities (audit logs to be made available for all the activities done through the inventory management tool)	Please provide more details for clarity.	It is clarified that the solution should log all changes in the Assets including application of patches.
354	111	Asset and Patch Management	8	The System should be able to do Inventory governance, including software (authorized and unauthorized) and hardware components.	software governance can be tracked and managed.. what how governance is needed, please clarify	It is clarified that the asset and patch status provides inputs for the IT governance.
355	112	Asset and Patch Management	17	The solution should support PCI compliance/ OVAL/ SCAP scan for integrated endpoints.	This is outside the asset management solution scope. Will be done by VA tools	Please refer to the amendment
356	113	VAS	11	It should cater to perform vulnerability scan of all IP devices present in their environment.	Please confirm the frequency of the scan to be performed as part of the VAS solution.	It is clarified that the scan should be performed whenever required by the bank.
357	113	VAS	11	The solution must have capability to perform active and passive asset discovery scan, network VA, database VA etc.	Please provide us the understanding on the number of assets / devices to be covered as part of this exercise. This will allow us to provide the appropriate effort required for this assessment.	It is clarified that the Vulnerability assessment solution is for finding vulnerabilities in the assets of the bank in ongoing basis to be done by the operational team. It is not a one time exercise.
358	113	VAS	11	The product must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.	Please confirm if the VAS Central manager can be accessible to all agents including remote users based on your network topology. This will help us to plan our implementation architecture	It is clarified that the access to the VAS central manager will be provided on need basis.

359	114	VAS	24	The proposed solution should provide mechanism to upload IP lists of devices through XLS format	In Text format, you can paste Ips. Request you to change as through XLS/Text Format	Please refer to the amendment
360	115	VAS	38	Should be appliance based	More clarity is required to understand	Please adhere to the specifications of RFP.
361	116	Commercial Bid	10	Security Incident and Event Management (SIEM) - 5000 EPS New Licenses, 1000 Device Licenses	Kindly clarify the 1000 device licenses mentioned here in the Commercial Bid template. The earlier sections of the RFP has only 5000 EPS for SIEM.	Please refer to the amendment
362	116	Commercial Bid	Table B - 8	Table B (CLMS) Multiplication factor of 200 Licenses.	Please allow to quote based on the number of devices.	IT is clarified that the bank has about 1000 devices
363	119	Blacklisting Clause	Annexure-I 1. BID FORM Compliance Terms and Conditions	We hereby undertake and agree to abide by all the terms and conditions including all Annexure, Corrigendum(s) etc. stipulated by the Bank in this RFP. Any deviation may result in disqualification of our bid. We understand & agree that in event of being successful in the bid, we shall comply to the terms & conditions of RFP in future and shall not attempt to get the same changed from Bank later on in process of implementation, contract signing, and extension of contract and / or subsequent purchase order/s from Bank. We understand and agree that such attempts and non-compliance to RFP terms may lead to cancellation of our Contract and suitable penal action may be taken by Bank against us including invoking the EMD and/ or PBG and blacklisting.	Request you to kindly delete the blacklisting and amend the clause as follows:*"We hereby undertake and agree to abide by all the terms and conditions including all Annexure, Corrigendum(s) etc. stipulated by the Bank in this RFP. Any deviation may result in disqualification of our bid. We understand & agree that in event of being successful in the bid, we shall comply to the terms & conditions of RFP in future and shall not attempt to get the same changed from Bank later on in process of implementation, contract signing, and extension of contract and / or subsequent purchase order/s from Bank. We understand and agree that such attempts and non-compliance to RFP terms may lead to cancellation of our Contract and suitable penal action may be taken by Bank against us including invoking the EMD and/ or PBG ~~and blacklisting~~."*	Please refer to the amendment
364	126	Pre-qualification CSOC Setup	Annx III	Please mention turnover* for last three financial years and include the copies of Audited Balance Sheet in support of it.	Kindly request to consider the last 3 financial years as FY2019-20, FY2020-21, FY2021-22. For FY 22-23 as the audit is still in progress.	It is clarified that unaudited balance sheet signed by company auditor for the years for which audited balance sheet is not available is accepted.

365	127	Performance Bank Guarantee	Annexure-IV	Performance certificate	Most of the customers are reluctant to provide the details in the format as asked in the annexure -IV. Hence we request to consider the details filled by the bidder in their letter head for the annexure IV, duly signed by the authorised signatory of the bidder. However bidder will attach the PO/LOI copy and completion certificate issued by the end user as part of supporting document.	It is clarified that the performance certificate can be produced by format in annexure/email from customer. If customer of the bidder is not willing to provide the performance certificate to the bidder and willing to be contacted by the bank, then Contact details of the customers need to be furnished to verify the performance.
366	129	Pre-qualification CSOC Setup	Annx VI	6. TURNOVER AND NETWORTH CERTIFICATE	Kindly request to consider the last 3 financial years as FY2019-20, FY2020-21, FY2021-22. For FY 22-23 as the audit is still in progress.	It is clarified that unaudited balance sheet signed by company auditor for the years for which audited balance sheet is not available is accepted.
367	139	Undertaking	Annexure XI	Annexure XI Undertaking of Information Security from the Bidder	This undertaking needs to be provided by the respective OEMs. Bank to acknolwledge the same.	It is clarified that the undertaking is required from the bidder. However bidder may take required undertaking from the corresponding OEMs.

368	145	CHECKLIST FOR DOCUMENTS TO BE SUBMITTED WITH TECHNICAL BID	4	PERFORMANCE CERTIFICATE & PO SUPPORTING THE CLAIM FROM THE RESPECTIVE ORGANIZATION SHOULD BE SUBMITTED ALONG WITH CONTACT DETAILS OF THE COMPANY.	Request bank to accept self-declaration along with artifact eg(PO, signoff, and Performance certificate used for Indian Bank Bid) Justification: It becomes very difficult for SI to reach out to any customer multiple times just to ask for feedback.	It is clarified that the performance certificate can be produced by format in annexure/email from customer. If customer of the bidder is not willing to provide the performance certificate to the bidder and willing to be contacted by the bank, then Contact details of the customers need to be furnished to verify the performance.
369	145	Checklist	7	THE BIDDER MUST HAVE THEIR CAPTIVE SOC FOR LAST 5 YEARS IN INDIA PROVIDING SECURITY SERVICES TO VARIOUS PUBLIC/PRIVATE COMPANIES/ORGANISATIONS.	Request to remove this clause	Please refer to the amendment
370	145	Pre-qualification CSOC Setup	Annx XV, Pt 5	AUDITED FINANCIAL STATEMENTS FOR THE LAST THREE (3) FINANCIAL YEARS I.E., FY2020-21, FY2021-22 & FY2022-23	Kindly request to consider the last 3 financial years as FY2019-20, FY2020-21, FY2021-22. For FY 22-23 as the audit is still in progress.	It is clarified that unaudited balance sheet signed by company auditor for the years for which audited balance sheet is not available is accepted.
371	-	Topology/ Network details of RRB's	-	General	Describe the topology of the network - capturing the infrastructure and security components, with the connectivity between DC and DR. Also, Please confirm if any other location has to be considered for this implementation	It is clarified that the details will be provided to successful bidder.
372	-	General	-	General	Any specific compliance requirement to be followed. If so, please list it down.	It is clarified that the compliance to GOI, Cert-In, RBI, NABARD and any other regulatory bodies of the bank to be followed

373	-	ITSM tool	-	General	Please share the current ITSM tool available within the bank environment. If we don't have one, can LTTS propose the solution as part of this RFP	It is clarified that currently bank is in the process of procuring the ITSM tool and it is not a part of this RFP
374	21-27	LIQUIDATED DAMAGES & SLA	26. Liquidated Damages	LIQUIDATED DAMAGES & SLA	We would like to modify as follows:- TC'S SOLE LIABILITY AND TNGB 'S SOLE REMEDY FOR DAMAGES ARISING OUT OF OR RELATING TO ANY ACT OR OMISSION RELATING TO THE FURNISHING OF OR THE FAILURE TO FURNISH SERVICES (INCLUDING BUT NOT LIMITED TO MISTAKES, OMISSIONS, INTERRUPTIONS, FAILURE TO TRANSMIT OR ESTABLISH CONNECTIONS, FAILURE TO SATISFY SERVICE LEVELS OR SPECIFICATIONS, DELAYS, ERRORS OR OTHER DEFECTS) IS LIMITED TO ANY APPLICABLE CREDIT ALLOWANCES DUE AND/OR TNGB'S RIGHT TO TERMINATE A PARTICULAR SERVICE UNDER THE APPLICABLE SERVICE LEVEL GUARANTEE AS SET FORTH IN THE RELEVANT SERVICE SCHEDULE(S).	Please adhere to the terms and conditions of the RFP
375	Additional Query	Internal Firewall	Internal Firewalls	Gateway Management	Please clarify if VM based or Appliance Based management is required	It is clarified that VM based management is required.
376	Additional Query	Internal Firewall	Internal Firewalls	Requrement of Sandbox for Internal Firewall	Since it is internal, please clarify if Sandboxing is required or not. If not, the please remove Zero day and Sandboxing Line items. If Yes, please specify if On Prem Sandboxing is required or cloud based and the mode of deployment. We recommend to have sandbox in integration mode.	It is clarified that sandboxing is not required for internal firewall.
377	Additional Query	Internal Firewall	Internal Firewall	Gateway Management	Please clarify if VM based or Appliance Based management is required	It is clarified that gateway management is VM based.
378	Additional Query	Internal Firewall	Internal Firewall	Requrement of Sandbox for Internal Firewall	Since it is internal, please clarify if Sandboxing is required or not. If not, the please remove Zero day and Sandboxing Line items. If Yes, please specify if On Prem Sandboxing is required or cloud based and the mode of deployment. We recommend to have sandbox in integration mode.	It is clarified sandboxing is not required for Internal firewall
379	Additional Query	Arcon			Are they looking for Perpetual Based AMC or Subscription Based AMC?	Please refer to the amendment
380	Additional Query	Arcon			As in the RFP it is clearly stated that the Bank is having 50 existing User Licenses, Please check what is the Device Count? , Please check what is the Device Count?	Please refer to the amendment

381	Bid Submission Timelines	Bid Submission Timelines	Bid Submission Timelines	Bid Submission Timelines	Requesting the Bank to consider extending the Bid Submission Timelines to at least 6 weeks from the date of receipt of the Pre-bid responses from the Bank.	It is clarified that the details of bid submission timelines will be published in GeM portal
382	nil	WAF	4	Additional request	Requesting the Bank to add the following clauses: 98. The platform must support following persistance profile cookie, dest-addr,has, host,sip, source-addr, ssl, universal (extract any data networm, app protocol, payload) 99. The platform must support all intelligent load balancing methods including; round robin, least connection, ratio, observed , predictive dynamic, fastest. 100. The solution should support scripting rules to modify the flow of traffic from Layer-4 to Layer-7. It should also support adding, modifying, removing L7 headers and payload if required to make the application fucntionality working.	Please adhere to the specifications of RFP.
383	nil	SIEM	56	General Query	Kindly clarify whether the SIEM Solution mentioned should be in High Availability or Not.	It is clarified that HA is not expected for SIEM
384	nil	General	General	General Query	Request Details on Application /Hrdware Appliance to be Upgraded	It is clarified that upgradation of PIM solution is required.
385	nil	General	General	General Query	Could you please share the details of the existing security solutions to be managed?	It is clarified PIM Solution has to be managed.
386	nil	General	General	General Query	Request Details on Existing License	It is clarified that the details are mentioned in the RFP
387	nil	MII	General	General Query	Since Make in India Clause involved request to relax this Clause	Please adhere to the terms and conditions of RFP
388	nil	Pre-qualification CSOC Setup	General	General Query	Request to Amend -The bidder should be providing SOC services in customer premises with SIEM of 5000 EPS for minimum two customers on or before 31/03/2021 and should continue to provide the service to the customers as on 31/03/2023-	Please adhere to the terms and conditions of RFP
389	nil	Payment Terms	General	General Query	Request to Amend Payment Terms-On Delivery-80 % of A & 80 % of E	Please refer to the amendment
390	nil	Payment Terms	General	General Query	Request to Amend Delivery Period- 12 to 15 weeks from date of PO	Please adhere to the terms and conditions of RFP

391	nil	PIM	ARCON PAM	General Query	1. As in the RFP it is clearly stated that the Bank is having 50 existing User Licenses, Please check what is the Device Count?	Please refer to the amendment
392	nil	PIM	ARCON PAM	General Query	2. Are they looking for Perpetual Based AMC or Subscription Based AMC?	It is clarified that Perpetual license is available now
393	nil	Merger and Acquisition clause	General	New clause	A bid submitted by a Bidder who has acquired a Company/Division/Business Unit of its parent organisation shall also be considered for evaluation if the eligibility criteria and technical evaluation criteria is met jointly by the bidder and its parent Company. Document Proof: Business Transfer Agreement (BTA) or Board regulation of both company	It is clarified that the bidder may submit the relevant documents as proof of Acquisition
394	nil	Man Power	General Query	General Query	Please confirm Security Incident Management and Monitoring is out of scope. Output of SIEM, EDR & DLP incidents and alerts management is out of scope.	It is clarified that all incident managements are in scope
395	nil	Internal& External Firewall	Internal& External Firewal	General Query	Can we have a single management server for both DC & DR. The Firewall solution shall support configuration of firewalls\enforcement modules from management consoles installed in different device only	It is clarified that management server should be setup in both DC & DR
396	nil	Internal& External Firewall	Internal& External Firewall	Is there any existing Firewall present as external & should we migrate the configurations?	General	It is clarified that migration of configuration is not required
397	nil	WAF	New RFP Clause	New RFP Clause	The platform must support following persistance profile cookie, dest-addr,has, host,sip, source-addr, ssl, universal (extract any data networm, app protocol, payload). Request bank to include this point as Wide range of persistance profiles is required to have common integration from multiple services.	Please adhere to the specifications of RFP.
398	nil	WAF	New RFP Clause	New RFP Clause	The platform must support all intelligent load balancing methods including; round robin, least connection, ratio, observed , predictive dynamic, fastest.. Request bank to include this point as Wide range of load balancing method is rquired to achieve the required use case based on customer environment.	Please adhere to the specifications of RFP.
399	nil	WAF	New RFP Clause	New RFP Clause	The solution should support scripting rules to modify the flow of traffic from Layer-4 to Layer-7. It should also support adding, modifying, removing L7 headers and payload if required to make the application fucntionality working.Request bank to include this point as Today most application required few modification to be done at the L7 header to comply to security and to achieve application functionality.	Please adhere to the specifications of RFP.

400	nil	Non-solicitation	New RFP Clause	New RFP Clause	Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.	Please adhere to the terms and conditions of RFP.
401	nil	Retention of copies	nil	Retention of copies	On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied. bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.	Please adhere to the terms and conditions of RFP.
402	nil	Non-Exclusivity	nil	Non-Exclusivity	It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Please adhere to the terms and conditions of RFP.
403	nil	Patch Management	Patch Management General Queries	New RFP Clause	How many named technicians need access to the Patch Management Solution? How many remote sites/offices are to be managed and are they interconnected Can we have the bifurcation of workstations and servers from the 5500 endpoints Please clarify if all these 5500 endpoints are AD integrated or if the Bank has workgroup machines as well	1 - About 20 technicians need access to the patch management console. 2 - Bank has about 1000 locations and all are connected to central site 3 - No of workstations and servers to be identified by the asset management solution. 4 - All endpoints are integrated to AD.
404	nil	SIEM	SIEM	General Query	Expected number of devices to be integrated with SIEM	IT is clarified that about 500 devices are expected to be integrated with SIEM. However, licenses should be based only on EPS

405	nil	SIEM	SIEM	General Query	Expected number of applicattions to be integarted with SIEM	It is clarified that the details will be provided to successful bidder.
406	nil	SIEM	SIEM	General Query	Name locations where the devices /application servers are present.	It is clarified that the details will be provided to successful bidder.
407	nil	SIEM	SIEM	General Query	Data retention period.(Number of months/years)	It is clarified that the data retention period is as per policy of the bank. Currently it is one year.
408	nil	SIEM	SIEM	General Query	Why separate CLMS is considering as the same functionality is achieved via SIEM?	It is clarified that SIEM is expected to analyse information security logs and CLMS is expected to hold all logs without analytics.
409	nil	WAF	WAF	General Query	Number of applications to be protected by WAF.	It is clarified that no of applications is not limited.
410	nil	WAF	WAF	General Query	Any existing WAF solution is present. Should we migrate the configurations?	It is clarified that migration is not required
411	nil	Man Power		General query	Our understanding is that end user related queries will not be part of the scope of FMS and the same would be supported by the helpdesk team of the bank. Kindly confirm.	It is clarified that the end user related queries for in scope solutions are part of FMS of this bid
412	nil	ITSM tool		General query	Monitoring and ITSM tool. Kindly confirm if the bank would provide the monitoring and ITSM tool for monitoring and ticketing purposes. Also, from ITSM tool perspective, since three RRBs are involved, our recommendation is to have one common ITSM. Pls confirm on this.	It is clarified that the bank is in process of procuring the ITSM Tool.

413	nil	DC/ DR Locations		General query	Within the duration of the contract kindly confirm if there are any plans for the bank to change the location of the DC / DR / Other critical locations. If yes, under such scenarios the resinstallation / redployment of the solutions and resources in the new locations will be treated as a separate change request project.	It is clarified that such changes will be discussed with the successful bidder and will come under change management.
414	Page 40	REQUIREMENT OF MAN POWER		L2 onsite resource at DC/DR Other Locations as specified by Bank	Need Clarification. L2 onsite resource at DC/DR Other Locations as specified by Bank are 24x7x365 or in General shift	It is clarified that L2 resources should work from 0800 hrs to 2000 hrs in shift. Bank holidays list may be downloaded from Indian bank's website. (i.e) www.indianbank.in.
415	SIEM	SIEM		The proposed solution should be sized for 5,000 sustained EPS at correlation layer initially per Data centre but should be able to handle peak >License deployed EPS (additional 5000 EPS to take care of spikes/	Please confirm on the total data centers in scope for SIEM to size the comlpete solution, going by the propotion of 5000 EPS per data center	The requirement is expected for two Data centers