RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
1.2	5	Earnest Money Deposit by RTGS/NEFT	INR 10,00,000/- (Rupees Ten Lakh Only) RTGS/NEFT Details: A/c. no. : 017511029000129, IFSC: AHDC0000175, A/c Name:- Ahmednagar District Central Cooperative Bank Ltd, Branch: Head Office	We request to modify the clause as below:- INR 10,00,000/- (Rupees Ten Lakh Only) BG from any Scheduled Commercial Bank / RTGS/NEFT Details: A/c. no. : 017511029000129, IFSC: AHDC0000175, A/c Name:- Ahmednagar District Central Cooperative Bank Ltd, Branch: Head Office	RFP Requirement stands
2	7		Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services (as service)	**Request to calrify below :** Kindly provide the number of Domians and subdomains which needs to be cover under this service.	Kindly refer RFP's Annexure 11
8	8	2 (Table)	Dark Web Monitoring (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services	Please provide the number of primary internet domains, external IP ranges, and the number of VIP/Executive profiles to be actively monitored under the Brand Protection and DWM services.	Kindly refer RFP
2	8	1 to 10	Bank expects below solutions to be provided as part of SOC with the management & monitoring will cover all devices & solutions already implemented at bank's end. • Security Information & Event Management (SIEM) (as service) • Extended Detection and Response (XDR) • Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services (as service) • Database activity monitoring (DAM), • Privileged identity and Access management (PIM/PAM) • Data Loss Prevention (DLP) • Patch Management as a service. • Web Application Firewall (WAF) • Perimeter Firewall. • Network Behavior Anomaly Detection (NBAD)	**Request to calrify below :** Quantity is not given for required solutions. Request to provide the quantity and specification for required security controls	Kindly refer RFP's Annexure 10 and 11
2	9		Bidder should have 24*7*365 back-to-back support with OEM during the total contract period for necessary support.	**Request to note below / modify :** This shall be applicable and can be provided for On-prem physical Applinacve Solution, if supplied.	RFP Requirement stands
2	9		Time Schedule of the Project	**Request to calrify below :** Kindly provide the Go live period.	Kindly refer RFP
2.1	10	4	"Bidder to provide the connectivity along with bandwidth from Bank's DC to CSOC DC and DR in redundant mode..."	Does the Bank have a minimum required bandwidth (e.g., in Mbps), or is the bidder expected to calculate this entirely based on anticipated log volume?	Understanding is correct, bidder to propose the required bandwidth (for entire project tenure) based on the location and required services.
2.1	10	6	The Bank intends to have various modules of CSOC solutions placed in DC to be in HA (High Availability) mode, also the Bank intends to have CSOC solutions in DR in standalone mode for redundancy.	Kinldy clarify if the support centre remote/branch location mentioned in the asset list is in scope. If yes, then will it be a HA or standalone deployment	Yes, Stand alone
2.1	10	2	CSOC shall conduct deep scan of packets including secure traffic passing through internet/ web gateway of the Bank and shall use the intelligence to correlate with other logs and generate meaningful reports / alert.	**Request to calrify below :** Kindly elaborate the term deep scan of packets and its requirement details.	"Deep scan of packets" means closely examining network data (even secure traffic using safe methods like metadata or controlled decryption at the gateway) to understand what is happening, link it with other security logs, and raise useful alerts or reports.
2.1	10	4	Bidder to provide the connectivity along with bandwidth from Bank's DC to CSOC DC and DR in redundant mode and Bank's DR to CSOC DC and DR in standalone.	**Request to calrify below :** Kindly confirm if we need to provide separate internet connectivity for this or existing bank internet connectivity can be used. We can connect CSOC DC & DR over Internet using IPSEC tunnel.	Kindly refer RFP
2.1	11	8	"Assets to be integrated for CSOC: ... Branch Desktop 2000, Branch Router 299..."	What is the Bank's current or estimated Events Per Second (EPS) requirement to accurately size the SIEM log collectors and storage capacity?	SIEM is presently not available in Bank. Bidder to analyze and propose the required EPS (for entire project tenure) based on the provided asset details with their experties.
2.1	11	13	The proposed backup target should be disk based hardware solution.	Please confirm do we need to provide new backup solution for the proposed CSOC solution at DC or DR.	Kindly refer RFP
2.1	11		Assets to be integrated for CSOC:	**Request to calrify below :** Kindly provide the OEM details of devices which needs to be integrated with CSOC	This data will be shared with final selected bidder

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
2.1	11	16	Anti-Virus and HIPS	**Request to calrify below :** Need make and model of existing Anti-Virus and HIPS. Alos, please clarify if existing Anti-Virus and HIPS will run paralally or need to be removed.	This data will be shared with final selected bidder
2.1	11	9	Email solution along with Security	**Request to calrify below :** Need make and model of existing Email solution, along with Security for SIEM integration.	This data will be shared with final selected bidder
2.1	12	31	"Bidder should provide Forensic support for 50 Hours per year and it will be on actual basis based on hours spent in a year."	Does the Bank require the bidder to provide specialized third-party forensic tools and investigators for this, or will this be conducted using the proposed CSOC solutions by the L2/L3 analysts?	Investigations are expected to be performed by the bidder's L2/L3 analysts using the forensic and investigative capabilities embedded within the proposed CSOC solutions, with third-party forensics required only in exceptional regulatory or legal scenarios
2.1	14	50	Solution should cover Phishing simulation and training module to educate bank users and test their response to phishing attacks.	**Request to calrify below :** Kindly provide the number of users for Phishing simulation and training module	Total 1500 no.of users
2.2	15		24*7*365 monitoring of CSOC solution at ADCC.	**Request to calrify below :** Kindly confirm if onsite resources need to monitor 24*7*365 or remote monitoring require	Kindly refer RFP
2.2	16		The onsite resources should fulfill the below minimum criteria	**Request to calrify below :** Please define the number of shifts and resources per shift	Kindly refer RFP
	16		Onsite CSOC Management during banking hours	**Request to calrify below :** Kindly confirm if onsite resources need to monitor 24*7*365 or remote monitoring require	Kindly refer RFP
3.1	17	A4	The Bidder should have its own managed Cyber SOC along with a DR site located in a different seismic zone within India.	We request to modify the clause as below:- The Bidder should have its own managed Cyber SOC along with its DR site in India.	RFP Requirement stands
3.1	17	C1	The bidder should have prior experience of the Implementation & management of CSOC for at least Three (3) State/District Co-operative Banks in India in the last 5 years.	We request to modify the clause as below:- The bidder should have prior experience of the Implementation & management of CSOC for at least Three (3) State/District Co-operative Banks/ Schedule Commercial /PSU Bank in India in the last 5 years.	RFP Requirement stands
3.1	17	1	The bidder must be a Government Organization / PSU / PSE or a Public / Private Limited Company or a partnership firm incorporated in India and operating in India for at least 5 years as on date of the RFP.	**Request to consider below :** In case the bidding company/firm is hived off from the demerged company, the experience, eligibility etc as per the requirement of the RFP may be considered as of the demerged company, provided the demerged company doesn't apply in the same RFP process. If the bidder is a 100% owned subsidiary of its parent company, the experience and eligibility requirements may be considered based on either the bidder or its parent company. If the bidder is a wholly owned parent company of a subsidiary, the experience and eligibility requirements may be fulfilled based on either the parent company or its subsidiary.	RFP Requirement stands

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
3.1	17	C. 3	Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM.	We request you to amend the cllause as: "Bidder should have at least 10 IT resources having certifications in CISA / CEH / CISSP / CISM / CRISC / ***CompTIA Security+ /OSCP*** , or professionally certified from OEMs on proposed major solutions such as SIEM." We request inclusion of **C*ompTIA Security+ and OSCP certifications*** , as these are globally recognized, highly relevant, and competitive cybersecurity certifications that align with the technical scope of the proposed project requirements. The inclusion of ***CompTIA Security+ and OSCP*** in the approved certifications list will broaden the eligibility criteria to reflect current industry standards, encourage wider participation from qualified vendors, and ultimately serve the best interests of ADCC Bank by attracting the most competent and experienced service providers.	RFP Requirement stands
3.1	18	C4	Service Model: The bidder should provide the CSOC services from MeitY empaneled cloud infrastructure i.e., SIEM / DLP/PIM etc., Solution should be hosted with MeitY empaneled cloud.	We request to accept Certificate / website proof.	RFP Requirement stands
3.1	18	C6	**Each of the proposed solutions** should have been supplied for at **least three (03) Cooperative Bank**(DCCBs/ State/Urban Cooperative) Bank in India. 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	We request to modify the caluse as below:- Each of the proposed solutions should have been supplied for at least three (03) Cooperative Bank(DCCBs/ State/Urban Cooperative)/Scheduled commercial / PSU Bank in India. 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	RFP Requirement stands
3.1	18	6	Each of the proposed solutionsshould have been supplied for at least three (03) Cooperative Bank(DCCBs/ State/Urban Cooperative) Bank in India. 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	Kindly ammend this clause to : Each of the proposed solutionsshould have been supplied for at least three (03) Cooperative Bank(DCCBs/ State/Urban Cooperative) **or BFSI/ Finance Department/Govt department** in India. 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	RFP Requirement stands

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
3.1	18	6	Each of the proposed solutions should have been supplied for at least three (03) Cooperative Bank(DCCBs/ State/Urban Cooperative) Bank in India. 1. Security Information & Event Management(SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM) 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management(PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	**Request to modify:** Atleast 5 of the below proposed solutions should have been supplied for at least three (03) Banks in India. 1. Security Information & Event Management(SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall (WAF) 6. Database activity monitoring (DAM) 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management(PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD)	RFP Requirement stands
3.1	18	6	Patch Management as a service	**Request to note below / modify :** Patch Management is not a Security Product, but falls yunder Compute / Infra / PaaS management activities.	RFP Requirement stands
3.1	18	6	Extended Detection and Response (XDR)	**Request to calrify below :** EDR and XDR are separate functionality. Kindly clarify if EDR is desired or XDR.	Kindly refer RFP
3.1	18	6	Perimeter Firewall	**Request to calrify below :** Kindly provide the detailed spesifications and quantity.	Kindly refer RFP's Annexure 10
4.5	21	3 Bidder's capability and experience (Maximum Marks 40)	➢ The bidder should have prior experience of the Implementation & management of CSOC for at least Three (3) Cooperative Banks in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for Five (05) or more Cooperative banks in India out of which Two (2) should be State Cooperative or DCCB in the last 5 years. b. 7 Marks: If the bidder provides credentials for at least Three (03) Cooperative bank in India in the last 5 years.	We request to modify the clause as below:- ➢ The bidder should have prior experience of the Implementation & management of CSOC for at least Three (3) Cooperative / Scheduled commercial / PSU bank in India in the last 5 years. a. 10 Marks: If the bidder provides credentials for Five (05) or more Cooperative /Schedule Commercial / PSU Bank in India out of which Two (2) should be State Cooperative or DCCB in the last 5 years. b. 7 Marks: If the bidder provides credentials for at least Three (03) Cooperative /Schedule Commercial / PSU bank in India in the last 5 years.	RFP Requirement stands

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
4.5	21	3 Bidder's capability and experience (Maximum Marks 40)	➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a Cooperative bank in India in the last 5 years. a. **10 Marks**: If the bidder provides credentials for at least **Eight (8) from the below- proposed solutions in one Cooperative bank in India in the last 5 years.** b. **7 Marks:** If the bidder provides credentials for at least Six (6) from the below- proposed solutions in one Cooperative bank in India in the last 5 years. **The proposed solutions are:** 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall(WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD) **Note:** If the bidder does not have a single credential mentioning above all components in a bank, the bidder is free to provide credentials from at least one bank for each of the identified components separately which includes SIEM.	We request Bank to accept multiple PO for different solution. We request to modify the clause as below:- ➢ The bidder should have prior experience in the Implementation of the mentioned solutions in a Cooperative/Schedule Commercial / PSU bank in India in the last 5 years. a. **10 Marks**: If the bidder provides credentials for at least **Seven (7) from the below solutions in one Cooperative/Schedule Commercial / PSU bank in India in the last 5 years.** b. **7 Marks:** If the bidder provides credentials for at least Four (4) from the below solutions in one Cooperative / Schedule Commercial / PSU bank in India in the last 5 years. **The solutions are:** 1. Security Information & Event Management (SIEM) 2. Extended Detection and Response (XDR) 3. Patch Management as a service 4. Dark web Monitoring & Brand Protection (DWM) along with Anti-Phishing, Anti-Trojan, Anti-Malware, Anti-rouge services 5. Web Application Firewall(WAF) 6. Database activity monitoring (DAM), 7. Data Loss Prevention (DLP) 8. Privileged identity and Access management (PIM/PAM) 9. Perimeter Firewall 10. Network Behavior Anomaly Detection (NBAD) **Note:** If the bidder does not have a single credential mentioning above all components in a bank, the bidder is free to provide credentials from at least one bank for each of the identified components separately which includes SIEM.	RFP Requirement stands
4.5	22	3 Bidder's capability and experience (Maximum Marks 40)	➢ Bidder should have currently in the business of providing CSOC/ SOC managed security services including log monitoring and correlation for minimum **50 assets and 1000 EPS in at least two(2) Cooperative Banks in India.** a. **10 Marks:** If the bidder provides credentials for **three (03) or more Cooperative banks in India.** b. **7 Marks**: If the bidder provides credentials for at least two (02) Cooperative banks in India.	We request to modify the clause as below:- ➢ Bidder should have currently in the business of providing CSOC/ SOC managed security services including log monitoring and correlation for minimum **50 assets and 1000 EPS in at least two(2) Cooperative/Schedule Commercial/ PSU Banks in India.** a. **10 Marks:** If the bidder provides credentials for **three (03) or more Cooperative/Schedule Commercial/ PSU banks in India.** b. **7 Marks**: If the bidder provides credentials for at least two (02) Cooperative /Schedule Commercial/ PSU banks in India.	RFP Requirement stands
4.5	22	Sr. No.3	Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM a. 10 Marks: If the bidder provides declaration for more than 10 certified CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM resources under the company's payroll along with the CV and certificates. b. 7 Marks: If the bidder provides declaration for more than 5 and less than 10 certified CISA/ CEH/ CISSP/ CISM/ CRISC or professionally certified from OEM on proposed major solutions like SIEM resources under the company's payroll along with the CV and certificates.	We request you to amend the cllause as: Bidder should have at least 10 IT resources having certification in CISA/ CEH/ CISSP/ CISM/ CRISC***/ CompTIA Security+ /OSCP*** or professionally certified from OEM on proposed major solutions like SIEM a. 10 Marks: If the bidder provides declaration for more than 10 certified CISA/ CEH/ CISSP/ CISM/ CRISC***/ CompTIA Security+ /OSCP*** or professionally certified from OEM on proposed major solutions like SIEM resources under the company's payroll along with the CV and certificates. b. 7 Marks: If the bidder provides declaration for more than 5 and less than 10 certified CISA/ CEH/ CISSP/ CISM/ CRISC***/ CompTIA Security+ /OSCP*** or professionally certified from OEM on proposed major solutions like SIEM resources under the company's payroll along with the CV and certificates.	RFP Requirement stands

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
	25	5.1	Availability of C-SOC Solution-99.98%	**Request to calrify below :** Request to amend clause as " Availability of C-SOC Solution-99.9%"	RFP Requirement stands
5.3	26	5.3	Resolution time of helpdesk- 99.95%	**Request to calrify below :** Kindly check the seviarity mapping. Request to amend clause as " Resolution time of helpdesk- 95%"	RFP Requirement stands
6	39	6.31	**Renewal of Contract** In case ADCC Bank wants to continue with Bidder's services after the completion of this contract, Bidder shall offer the same services or enhanced services to ADCC Bank. Unless mutually agreed, the same rates shall apply.	**We propose to modify clause:-** Renewal of Contract In case ADCC Bank wants to continue with Bidder's services after the completion of this contract, Bidder shall offer the same services or enhanced services to ADCC Bank. ~~Unless~~ if mutually agreed, the same rates shall apply.	RFP requirement stands
6	39	6.3	**Effect of Termination** Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment. Reverse Transition mechanism would typically include service and tasks that are required to be performed / rendered by Bidder to ADCC Bank or its designee to ensure smooth handover (including data) and transitioning of ADCC Bank's deliverables, maintenance, removal of ADCC Bank's all data from the system/ cloud and facility management. Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services. The reverse transition phase shall be completed within 3 months. Bidder agrees that after completion of the Term or upon earlier termination of the assignment Bidder shall, if required by ADCC Bank, continue to provide maintenance services to ADCC Bank at no less favorable terms than those contained in this document. In case ADCC Bank wants to continue with Bidder's services after the completion of this contract then Bidder shall offer the same or better terms to ADCC Bank. Unless mutually agreed, the rates shall remain firm. Bidder agrees that ADCC Bank at any point of time during tenure of contract may return/discontinue any of the Deliverables/services in whole or part thereof offered under this document. ADCC Bank shall not be liable to make any payment in respect of the Deliverables/services returned in whole or part thereof.	**We propose to modify:-** **Effect of Termination** Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment for a period of one (1) year. Reverse Transition mechanism would typically include service and tasks that are required to be performed/ rendered by Bidder to ADCC Bank or its designee to ensure smooth handover (including data) and transitioning of ADCC Bank's deliverables, maintenance, removal of ADCC Bank's all data from the system/cloud and facility management. Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services. The reverse transition phase shall be completed within 3 months subject to ADCC Bankl providing timely acess, approvals, and resources for necessary completion. Bidder agrees that after completion of the Term or upon earlier termination of the assignment Biddershall, if required by ADCC Bank, continue to provide maintenance services to ADCC Bank at no less favorable terms than those contained in this document. In case ADCC Bank wants to continue with Bidder's services after the completion of this contract then Bidder shall offer the same or better terms to ADCC Bank. ~~Unless~~ If mutually agreed, the rates shall remain firm. Bidder agrees that ADCC Bank at any point of time during tenure of contract may return/discontinue any of the Deliverables/services in whole or part thereof offered under this document. ADCC Bank shall not be liable to make any payment in respect of the Deliverables/services returned in whole or part thereof.	RFP Requirement stands
6.39	43	6.39	The proposed rate of penalty is as mentioned in Service levels with an overall aggregate cap of penalty to be limited to 10% of contract value.	Can we have Aggregate Cap of Penalty amount as 5% of contract value? We request to modify the clause as below:- The proposed rate of penalty is as mentioned in Service levels with an overall aggregate cap of penalty to be limited to 5% of contract value.	RFP Requirement stands
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the complete OEM details (Make/Model/Version) of the existing: - Firewalls (DC, DR, Branches) - Core Switches - L3 Switches - Routers - Load Balancers - WAF - Proxy - NAC - VPN Gateway - Mail Gateway - Existing Security Solutions integrated with SOC This is required to validate NBAD compatibility and flow export support (NetFlow, IPFIX, sFlow, JFlow, NSEL etc.).	Detailed OEM make/model/version information is strictly confidential not required at the pre-bid stage for an NBAD solution, as compatibility can be validated through confirmation of supported standard flow export protocols for (NetFlow/IPFIX/sFlow, etc.). These details will be shared with final selected bidder.

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	Please confirm whether separate dedicated network TAP/SPAN ports will be provided by the Bank for NBAD traffic visibility at: - DC Site - DR Site - Support Center - Branch aggregation points (if applicable) Or should the bidder consider TAP procurement within scope?	Understanding is correct, bidder to considet TAP in proposed solution.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether customer has dedicated: - DC Site - DR Site - NDR/NOC/Support Center Site and whether firewall and switching infrastructure is available at all locations.	Yes
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** 1) Please confirm whether the customer has an existing SSL Decryption (SSLO) solution deployed. 2) If yes, kindly confirm the make/model, deployed throughput, and whether it is implemented at DC, DR, and other locations. 3) Additionally, please confirm whether the same SSL Decryption infrastructure can be leveraged for the NBAD solution to decrypt network packet traffic before analysis.	Currently, the solution in not deploymed in the Bank
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm if NBAD monitoring is required only for: - DC + DR or additionally for: - HO - Support Center - Branches - Internet Edge - SD-WAN Infrastructure	All mentioned
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the exact network throughput (average and peak) separately for: - DC Site - DR Site - NDR / Support Center Site This is required for accurate NBAD appliance sizing.	The details will be shared with final selected bidder.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether traffic volume is same or distinct across: - DC - DR - NDR or whether traffic volume is distinct and independent for each location. Please share separate sizing parameters for each site.	Yes
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the average daily flow volume and expected peak concurrent sessions for: - North-South traffic - East-West traffic - Branch traffic - Internet traffic - Inter-DC traffic	The details will be shared with final selected bidder. Meanwhile, bidder to calculate & propose for a bank with 300+ branches based on their similar experience.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether encrypted traffic analytics (ETA) is mandatory for SSL/TLS encrypted traffic inspection and if SSL decryption infrastructure already exists.	Encrypted Traffic Analytics (ETA) is not mandatory for the NBAD solution, as it can analyze encrypted traffic using metadata without decrypting SSL/TLS traffic. Bidder may propose ETA based on the proposed architecture.

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the total internet bandwidth and MPLS/SD-WAN bandwidth currently available at: - DC - DR - Branches for accurate NBAD planning.	Kindly Refer Internet Bandwidth- DC: 20 Mbps DR: 20 Mbps Support Center: 30 Mbps Head Office: 20 Mbps Branches: 2Mbps SD-WAN Bandwidth- DC: 1Gbps DR: 1 Gbps Support Center: 15 Mbps Head Office: 100Mbps Branches: 8Mbps
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether customer requires: - HA for all NBAD components at DC - Standalone deployment at DR or - HA deployment at both DC and DR locations.	Kindly refer RFP for the deployment methodology.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether Active-Active or Active-Passive HA architecture is expected for NBAD at DC.	NBAD will be deployed at the Data Center in either an Active-Active or Active-Passive high-availability architecture.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the expected RPO and RTO requirements for NBAD in case of DC failure.	The desired RTO is 90 Mins and RPO is 30 Mins.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether separate storage for 30 days retention must be available individually at: - DC - DR or centralized retention is acceptable.	This clause will be applicable if bidder proposes hardware based NBAD, kinldy refer Annexure:10 for better understanding.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the required online retention and archival/offline retention period for the NBAD solution.	The solution shall ensure at least 30–90 days of online, searchable flow and analytics data, with archival/offline retention ranging from 6 to 12 months, as per best-practice guidelines
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm the exact DC-DR replication bandwidth required for NBAD metadata replication and whether the Bank will enhance the existing replication link accordingly. (RFP mentions bidder to confirm capacity and bank will enhance accordingly.)	The bidder is required to recommend the necessary bandwidth for replication of the proposed solution

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether integration with the following is mandatory from Day-1: - SIEM - XDR - Perimeter Firewall - WAF - DLP - PAM - DAM - Active Directory - DHCP - LDAP - RADIUS - Proxy - Threat Intelligence Platform - CERT-In / NCIIPC feeds or shall implementation be phased.	Understanding is correct, integration with components must be from Day-1
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether customer expects NBAD to provide: - Automated blocking via firewall - Quarantine VLAN enforcement - NAC-based isolation - SOAR-triggered response actions from Day-1.	Understanding is correct
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm expected growth factor beyond the mentioned 30% scalability from Day-1 for future commercial sizing across 5 years.	The bidder shall propose the expected growth factor, if it exceeds 30%, based on the proposed solution and architecture, to ensure appropriate sizing for a five-year period.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether historical packet forensics / packet capture (PCAP retention) is required as part of NBAD or only metadata/flow analytics is expected.	The bidder shall propose a best-fit, compliant solution in accordance with the RFP requirements.
8.10 Annexure 10: Functional and Technical Specification	61	1.7	**Annexure 10 - NBAD** Proposed NBAD systems should not have any dependency on existing switching infrastructure including but not limited to make, model, IOS, version etc.	**Request for Clarification:** Please confirm whether customer expects cloud workload traffic visibility (if any cloud workloads exist) as part of NBAD scope.	The bidder shall propose a best-fit, compliant solution in accordance with the RFP requirements.
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm the existing Endpoint Security solution deployed across the Bank, including: - Antivirus (AV) - Endpoint Detection & Response (EDR) - Host Intrusion Prevention System (HIPS) - Endpoint Protection Platform (EPP) Please specify OEM, product name, version, and deployment architecture.	Kindly refer below details -Antivirus (AV): Available at Bank - Endpoint Detection & Response (EDR): Not Available at Bank - Host Intrusion Prevention System (HIPS): Available at Bank - Endpoint Protection Platform (EPP): Not Available at Bank
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the existing AV/EDR/HIPS solution will be retained and integrated with the proposed XDR solution, or whether the bidder is expected to replace the existing solution completely.	Bidder to integrate the existing AV solution with proposed XDR.
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the customer has any existing OEM support contracts active for AV/EDR solutions and the current support validity period.	The existing Anti-Virus is covered with OEM Support till 31 March 2030

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm the exact number of: - Windows Servers - Linux Servers - AIX Servers - Virtual Machines - Physical Servers - End User Desktops - Laptops - Privileged User Systems - Domain Controllers - Database Servers - Critical Application Servers - Branch Endpoints - ATM/Micro-ATM endpoints (if applicable) for accurate XDR sizing.	Kindly refer RFP
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm the exact Operating System details for all endpoints and servers including: - Windows Server versions - Windows Desktop versions - Linux distributions and versions - AIX versions - VMware/Hypervisor versions - MAC OS This is required to validate agent compatibility.	The details will be shared with final selected bidder.
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether any legacy or End-of-Life operating systems are present in the environment, such as: - Windows XP - Windows 7 - Windows Server 2003 / 2008 - Old Linux kernels - Unsupported AIX versions Please provide approximate count for each.	The details will be shared with final selected bidder.
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether VDI, Citrix, Terminal Servers, shared jump servers, or thin-client environments are present and need XDR coverage.	Currently VDI, Citrix, Terminal Servers, shared jump servers, or thin-client environments in not available in the Bank
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the Bank has an existing centralized mechanism for automated agent deployment such as: - Active Directory (AD) - SCCM / MECM - Patch Management Solution - Software Deployment Tool - Endpoint Management Platform - GPO-based deployment - Existing EDR console deployment mechanism Please specify which system can be used for mass XDR agent deployment.	Currently, centralized mechanism in not deployed in the Bank except Active Directory(AD)
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the bidder can leverage the existing or proposed Patch Management solution for XDR agent push and lifecycle management.	Currently, centralized mechanism in not deployed in the Bank
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the customer expects: Automatic remote agent deployment or Manual deployment by bidder team especially for branch endpoints and remote systems.	Manual deployment

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether XDR scope includes: - Servers only - Endpoints only - Both Servers + Endpoints - Branch systems - ATM / Micro-ATM systems - Cloud workloads - SaaS applications (M365, Google Workspace etc.)	Endpoints and servers
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether XDR should include: - Email Security telemetry - Identity protection - Active Directory monitoring - Cloud workload protection - Network telemetry integration - Firewall telemetry - WAF integration - Proxy integration - IAM/PAM integration from Day-1.	Understanding is correct
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether mobile device security (Android/iOS) is part of XDR scope.	Mobile device security (Android/iOS) is not a part of XDR scope
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the customer requires ransomware protection, isolation, and automated response actions from Day-1.	Understanding is correct
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether internet access is available from all endpoints for cloud-managed XDR agents or if proxy-based communication is required.	Internet will not be provided
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether all branches are reachable centrally for remote deployment and monitoring via SD-WAN/MPLS.	Understanding is correct
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether XDR alerts must be integrated with: - SIEM - SOAR - Ticketing Tool - Email Alerts - Existing SOC workflows from Day-1.	Understanding is correct
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm expected future endpoint growth for the next 5 years for proper sizing and commercials.	10% to 20% Y-o-Y growth.
8.10 Annexure 10: Functional and Technical Specification	61	1	**Annexure 10 - XDR** The proposed solution should ingest logs from different channels of the Bank including but not limited to endpoints, servers, cloud, network and Active Directory to the vendor data lake for correlation, threat detection, threat hunting and response.	**Request for Clarification:** Please confirm whether the Bank requires on-premises XDR components only, or hybrid deployment with cloud-managed analytics is acceptable. (RFP mentions Analyzer in Managed SOC and Agents On-Premises.)	Kindly refer RFP
8.10 Annexure 10: Functional and Technical Specification	61	11	**DAM:** Track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed as a result.	We request to modify the clause as below:-Track execution of stored procedures, including who executed a procedure, what procedure name and when, as a result.	RFP Requirement stands

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
8.10 Annexure 10: Functional and Technical Specification	61	1	**DLP:**The DLP solution must have the capability of agent-less, cross-platform monitoring of outbound email activities, performed via corporate email.	**Note:** Any email DLP use cases covered by endpoint DLP will require Agent to be installed hence we request to modify the clause	RFP Requirement stands
8.10 Annexure 10: Functional and Technical Specification	61	8	**DLP**:Must be able to triger alerts for emails sent to high risk domains	**We request to modify the clause as below**:The solution should support policy-based monitoring and alerting for emails sent to high-risk or unauthorized domains, based on predefined or custom domain lists.**Or Request for Clarification**: Need details of Use case with details. beause This is more of an email security use case	Please consider the clause as deleted
8.10 Annexure 10: Functional and Technical Specification	61	6	**DLP:**Must show graphical summary of sensitive incidents detected by the Email Gateway	What Email GW and Email solution you are using? Need more detailed explination of this use case.	The details will be shared with final selected bidder.
Main Section - Annexure 10, Sub Section - SIEM		24	Service Provider should provide “canned” out-of-the-box reports for specific compliance regulations (PCI, SOX, GDPR) and control frameworks including, but not limited to NIST, COBIT, ISO Standards. This will be required based on ADCC Bank compliance requirements	COBIT is not a standard compliance mandated by RBI in its guidlines for the banking sector in India. Kindly ammend the clause to say: " Service Provider should provide “canned” out-of-the-box reports for specific compliance regulations (PCI, SOX, GDPR) and control frameworks including, but not limited to NIST and ISO Standards. This will be required based on ADCC Bank compliance requirements"	RFP Requirement stands
Main Section - Annexure 11, Sub Section - Software		1	Security Information & Event Management (SIEM) - Quantity 550	Kinldy elaborate on the quantity 550 mention in the BoM. Is the license quantity or any other metric?	Critical Asset Count
General Query	General Query	General Query	Network Behavior Anomaly Detection (NBAD)	Hardware-based deployments typically require procurement, delivery, and installation timelines. Please confirm if the bank is open to a software-based NBAD solution, which can significantly reduce deployment time and enable faster go-live and also reduse Cost.	Bidder may propose a colution in compliance ro RFP requirement(Hardware based or software based)
			Additional	**We recommend to incorporate a new clause under the RFP, which shall be mutually beneficial and significant in the context of business engagements :-** **Non-Solicitation:-** During the Term of this definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively, ""Representatives""). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	Additional clause not accepted.
			Additional	**It is recommended to include the below clause under the Termination section as follows:-** **Termination by the bidder for breach:-** In the event Bank materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the Bank, the bidder may terminate this definitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the Bank.	Additional clause not accepted.

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
			Additional	**It is recommended to include the below clause under the RFP:-** **Limitation of Liability:-** Notwithstanding anything to the contrary contained in this Agreement, the total aggregate liability of the Successful Bidder, whether arising in contract, tort (including negligence), strict liability or otherwise, shall not exceed the total fees/contract value paid or payable to the Successful Bidder under this Agreement. In no event shall the Successful Bidder be liable for any indirect, incidental, consequential, special, or punitive damages, including but not limited to loss of profits, loss of business, loss of data, or business interruption, even if advised of the possibility of such damages. The foregoing limitation shall not apply to (i) liability arising from fraud, gross negligence, or willful misconduct, or (ii) breach of confidentiality and data protection obligations, to the extent such exclusion is not permitted under applicable law.	Additional clause not accepted.
				What is the type of complaince that needs to be met by the customer by implementing PAM	All statutory/ regulatory compliances partaining to guidelines issued by RBI/ NABARD/CERT-IN/ MeitY etc.
				Are there any third party users/suppliers/contractors to whom the PAM access needs to be extended? If yes, kindly help us with the count.	Understanding is correct.
				How many number of privileged users are you looking for a PAM solution to be implemented	Kindly refer RFP's Annexure 11
				How many number of assets needs to be onboarded onto PAM	Kindly refer RFP's Annexure 11
				What are the kind of assets that needs to be integrated to the PAM	Kindly refer RFP's Annexure 11
				Is there a segregation between a normal access account and a privileged account	Understanding is correct
				What is the authentication source used by customer. For e.g. Active Directory, SAML etc	Active Directory is currently deployed and operational.
				What kind of deployment is customer looking for PAM. For e.g. Standalone, DC-DR, HA in DC-DR etc	Kindly refer RFP
				What kind of thick client based/exe based applications used by customer that needs to be onboarded onto PAM. Kindly help with the names of these applications if any.	The details will be shared with final selected bidder.
				Is there any IAM or MFA solution used by customer that needs to be integrated with PAM. If yes, kindly help us with the names	Currently, such solution in not deploymed in the Bank
				How many number of subsideries will the PAM solution will be extended to. Kindly help us with the count	Kindly refer RFP
				What kind of a deployment is the customer looking for ? For instance on-premises/cloud/hybrid	Kindly refer RFP
			Perimeter Firewall	Features required (FW, App Control, IPS, Anti Virus, Anti-Bot, IPS, Anti APT, URL Filtering.), Sandboxing, etc	Kindly refer Annexure 10
			Perimeter Firewall	No. of concurrent connections current & expected during peak hours	Kindly refer Annexure 10
			Perimeter Firewall	New connections per second	Kindly refer Annexure 10
			Perimeter Firewall	Expected throughput after enabling all security blades mentioned at point no. 4	Kindly refer Annexure 10
			Perimeter Firewall	Expected YOY % growth	Kindly refer Annexure 10
			Perimeter Firewall	VPN required (Site to Site)	Kindly refer Annexure 10
			Perimeter Firewall	No of VPN users (RA-VPN)	Kindly refer Annexure 10
			Perimeter Firewall	No of SSL VPN	Kindly refer Annexure 10
			Perimeter Firewall	Total Internet Bandwidth to be Terminated on firewall, considering future expansion	Kindly refer Annexure 10
			Perimeter Firewall	Total number of ISP links	Kindly refer Annexure 10
			Perimeter Firewall	Total MPLS Bandwidth to be Terminated on firewall, considering future expansion	Kindly refer Annexure 10
			Perimeter Firewall	What are major applications and SAAS/IAAS applications used (e.g. O365, AWS, Azure, etc)	Kindly refer Annexure 10
			Perimeter Firewall	No of users (Max in next three years)	Kindly refer Annexure 10
			Perimeter Firewall	Proxy/Web Gateway Used ?? Which one ?	Kindly refer Annexure 10
			Perimeter Firewall	Is Mail/Web/Application traffic passing.	Kindly refer Annexure 10
			Perimeter Firewall	Will Firewall Will be MTA ? If yes then number of incoming email per day and no of emails with attachment per day ? What is the max attachment size ?	Kindly refer Annexure 10

RFP No.: Computer/Tender/2026-27/001 Date: 21.04.2026					
Section Number	**Page Number**	**Point Number**	**Original Clause**	**Query**	**ADCC Bank Response**
			Perimeter Firewall	Type and no of interfaces require:	Kindly refer Annexure 10
			Perimeter Firewall	1GE RJ45 (Copper)	Kindly refer Annexure 10
			Perimeter Firewall	1GE SFP	Kindly refer Annexure 10
			Perimeter Firewall	10 GE SFP+	Kindly refer Annexure 10
			Perimeter Firewall	25G	Kindly refer Annexure 10
			Perimeter Firewall	40GE	Kindly refer Annexure 10
			Perimeter Firewall	100G	Kindly refer Annexure 10
			Perimeter Firewall	Is High-Availability required? (Active-Active, Active-Passive)	Kindly refer RFP
			Perimeter Firewall	Power Supply redundancy Required?	Kindly refer Annexure 10
			Perimeter Firewall	Is Firewall Hyperscale required ?	Kindly refer Annexure 10
			Perimeter Firewall	Expected firewall Throughput (performance) (MBPS/GBPS) with all required features enabled	Kindly refer Annexure 10
			Perimeter Firewall	HTTPS Interception required, mention the % of traffic for which SSL Inspection is required (e.g. 40 %, 70%, etc)	Kindly refer Annexure 10
			Perimeter Firewall	Is there a dedicated proxy/web gateway solution used for internet access of users/servers/workstations	Kindly refer Annexure 10
			Perimeter Firewall	Management Platform (HW Appliance or Software running on VM or SaaS based management)	Kindly refer Annexure 10
			Perimeter Firewall	Is Management server required in HA ?	Kindly refer Annexure 10
			Perimeter Firewall	Management Features Required? (Network Policy Management, Logging and Status, Compliance, Smart Provisioning, Monitoring, Management Portal, Smart Workflow, Smart Event, Smart Reporter Licenses.)	Kindly refer Annexure 10
			Perimeter Firewall	AI OPS, Policy Advisor, AI Policy Insights, AI Copilot required ?	Kindly refer Annexure 10
			WAF	No. of HTTP/S request per month?	The details will be shared with final selected bidder.
			WAF	Which feature you want us to enable CDN, DDoS, API Security, Gen AI security, Anti-bot?	Kindly refer Annexure 10
			WAF	Number of Applications?	The details will be shared with final selected bidder.
			WAF	Number of API calls?	The details will be shared with final selected bidder.