

Life Insurance Corporation of India – RFP/Tender for onboarding System Integrator (SI) to Implement Network Security Tools - Corrigendum-IV (LIC/CO/IT-BPP/NW/RFP/2023-2024/NS dated 06 February 2024)						
S.No.	RFP Section	Sub-Section	Pa No	RFP Clause	Bidder Query	LIC Response
1	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
2	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls and when required without adding overheads API-GW solution, promoting modern integration practices"	API Gateway and Security Solution has been removed from the scope of this RFP
3	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
4	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as web-sub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent"	API Gateway and Security Solution has been removed from the scope of this RFP
5	Annexure F - Technical Compliance	WAF Technical specs DC-DR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should be at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPS throughput? The difference is that when WAF devices does decryption as is the rightly the ask of the RFP it should publish numbers for HTTP and not HTTP on the Public datasheet.	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
6	Annexure F - Technical Compliance	WAF Technical specs DC-DR	19	The Proposed WAF should support 10 Gbps of WAF throughput and minimum 30000 RSA Per SEC (2048 BIT)/ECC.	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPS throughput? The difference is that when WAF devices does decryption as is it rightly asked in the RFP it should publish numbers for HTTP and not HTTP on the datasheet	WAF throughput, as stated in the datasheet, must reach 10Gbps, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
7	Annexure F - Technical Compliance	WAF Technical specs DC-DR	98	The solution should be able to block even the most advanced bots that try to emulate standard client behaviour and pretend to be web browsers.	Is LIC looking at Cloud based BOT mitigation service or on prem?	The WAF must be deployed on-premises as a hardware appliance, equipped with the capability to detect bots directly on the device. However, for more sophisticated bots, the WAF must include a feature to conduct additional inspection in the cloud, utilizing the same license. The integration between the WAF and the cloud-based bot engine must be seamless, ensuring that only header information is transmitted to the cloud-based bot for inspection, while the payload remains within the WAF and is not sent to the cloud-based bot engine.
8	Annexure F - Technical Compliance	WAF Technical specs NDR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should be at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	We request LIC to clarify the requirement of 10 Gbps WAF, is this HTTP or HTTPS throughput? The difference is that when WAF devices does decryption as is the rightly the ask of the RFP it should publish numbers for HTTP and not HTTP on the Public datasheet.	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
9	Annexure F - Technical Compliance	WAF Technical specs NDR	86	The solution must protect system against WASC Web Security Attack classification.	We request LIC to remove this point as WASC is outdated consortium the release was 12 years back. OWASP top 10 should be considered instead as it covers the latest attack types.	Please refer to the revised "Annexure F"
10	Annexure F - Technical Compliance	WAF Technical specs DC-DR	17	The proposed solution must support 10 Gbps of WAF throughput with minimum 128GB RAM. In case any OEM/bidder has WAF and load balancer in same appliance then the total L7 throughput should be at least be 200Gbps with minimum 192GB RAM or more. The bidder must provide evidence of throughput through publicly available documents at OEM websites prior to the date of RFP	Please clarify, is this HTTP or HTTPS throughput?	WAF throughput must meet a minimum of 10Gbps as outlined in the datasheet, specifically for HTTPS traffic. However, if the term "WAF throughput" is not explicitly stated in the datasheet, then the Layer 7 throughput should be 200Gbps or higher for HTTPS traffic.
11	Section C	Annexure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Annexure G"
12	Section H	Annexure F, 10		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS, TACACS+ or via local table of authorized users.	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS/TACACS+ / via local table of authorized users."	Please refer to the revised "Annexure F"
13	Section H	Annexure F, 86		The solution must protect system against WASC Web Security Attack classification.	Request to modify the clause as "The solution must protect system against WASC Web Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
14	Compliance			The CASB Solution must have HTTP/2 support from day 1.	This is Web Security (SWG) feature. It is requested to remove this clause.	Please refer to the revised "Annexure F"
15	Compliance			The CASB Solution must have 99% uptime SLA	Considering business applications access via Cloud Service Provider,SLA's for Cloud Vendor has to high. Our request to consider 99.999% uptime SLA instead of 99%	Please refer to the revised "Annexure F"
16	Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	This is SWG feature and not CASB feature. CASB is meant to protect SaaS applications and not vulnerabilities. This need SWG license consideration. Kindly relax the point.	Please refer to the revised "Annexure F"
17	Annexure F - Technical Compliance	NAC Technical Specification	65	The Proposed solution must have atleast 64GB RAM	Different Solution have various RAM requirement, for such a large requirement (1,27,000 endpoints), 64GB RAM may cause overall solution performance related issues. Request you to modify the clause as "The Proposed solution must have appropriate RAM so the overall solution will provide optimal performance across LIC network."	A minimum of 64GB RAM is required. However, the bidders may size it more as per the requirement.
18	Annexure F - Technical Compliance	NAC Technical Specification	67	The Proposed solution should provide comprehensive visibility of the network by automatically discovering, classifying, and enforcing policy for the endpoints connected to the network and must have capacity to enable the appropriate services for the total 1,27,000 endpoint devices scalable to 1,60,000 devices	LIC need 1,27,000 endpoint devices licenses and corresponding Hardware from day 1 and LIC will add additional Licenses and Hardware as and when require to meet the scalability of 1,60,000 devices, Does our understanding is correct?	The hardware has to be sized for 1,60,000 devices from day one. However, LIC may place the purchase order for the licenses in a staggered manner.
19	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____ (OEM) certifies that, the equipments being sold would not be declared End of Support (EoS) in the next 6 years and that _____ (OEM) shall supply suitable substitute in case EoS of equipments. Also _____ (OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no of years from 6 years to 5 years only for EoS and also from Support point of view. Most of the security solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
20	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera, IP Printers, IP Scanners etc. - IoT (IP Printer, IP Scanner, IP Phone, IP camera etc) Risk Assessment such as - Detect Insecure (TCP/UDP port open For example IP camera having Telnet Port open etc) - Detect IoT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	Requesting LIC to consider the point since LIC will have ~30% IoT devices which will not support traditional authentication method (such as Radius/DoTIX). It is not a good idea to only depend on 802.1x/MAC address bypass. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be update at any point in time to meet security aspect.	Please refer to the revised "Annexure F"
21	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera, IP Printers, IP Scanners etc. - IoT (IP Printer, IP Scanner, IP Phone, IP camera etc) compliance : The solution should be able to identify all network devices such as - Insecure (TCP/UDP port open For example IP camera having Telnet Port open etc) - IoT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	LIC will have ~30% IoT devices which will not support traditional authentication method (such as Radius/DoTIX). It is not a good idea to only depend on MAC address whitelists. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be update at any point in time to meet security aspect. Gartner 2021 Recommendation Gain visibility into on-premises infrastructure-connected devices with the goal of implementing access policies These devices include commonly used ones like workstations, laptops, printers, IP phones, IP cameras, access points, and IoT devices like OT, medical and building automation devices. Often, this motivation is driven by audit findings or an overall security strategy requiring authentication of all devices on a network.	Please refer to the revised "Annexure F"
22	Additional Points			The proposed solution must receive the SIEM data to take policy-based response actions such as quarantining or blocking potentially compromised or noncompliant devices, depending on the severity of the violation information received from SIEM. For example, SIEM detects, via firewall log correlation, a targeted denial of service (DoS) attack, it can direct proposed solution to have the Firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.	Gartner 2021 Recommendation Enable interoperability with other security solutions. This can be achieved in two ways: customization through open APIs or the use of built-in integration. NAC solutions increasingly feature anomaly detection capability to detect infected endpoints and MAC spoofing attempts on a network. However, integration with other security tools creates a better overall security context for an organization, which can be used to respond automatically to infected endpoints by quarantining them and thus preventing the spread of malware.	Please refer to the revised "Annexure F"
23	Additional Query				Please share total number of Network/L2-L3 devices i.e. Switches, Routers, Access Points, WLC, Firewall etc.	The details shall be shared with the successful bidder
24	Additional Points			Proof of Concept (POC) in Live environment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/ POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response per timelines stipulated from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in LIC environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"
25	-	-	-	-	With respect to MDM, need a clarity that can proposed solution be on cloud like SaaS offering with data residency in India. IBM Max360 is a SaaS Unified Endpoint Management solution offered by IBM that manages and protects any existing endpoint including laptops, desktops, mobile devices and apps, wearables, IoT and purpose built devices and allow protected, low risk access to company resources.	On Prem Solution is required
26	Annexure F - Technical Compliance	NAC Technical Specification	65	The Proposed solution must have atleast 64GB RAM	Different Solution have various RAM requirement, for such a large requirement (1,27,000 endpoints), 64GB RAM may cause overall solution performance related issues. Request you to modify the clause as "The Proposed solution must have appropriate RAM so the overall solution will provide optimal performance across LIC network."	A minimum of 64GB RAM is required. However, the bidders may size it more as per the requirement.
27	Annexure F - Technical Compliance	NAC Technical Specification	67	The Proposed solution should provide comprehensive visibility of the network by automatically discovering, classifying, and enforcing policy for the endpoints connected to the network and must have capacity to enable the appropriate services for the total 1,27,000 endpoint devices scalable to 1,60,000 devices	LIC need 1,27,000 endpoint devices licenses and corresponding Hardware from day 1 and LIC will add additional Licenses and Hardware as and when require to meet the scalability of 1,60,000 devices, Does our understanding is correct?	The hardware has to be sized for 1,60,000 devices from day one. However, LIC may place the purchase order for the licenses in a staggered manner.
28	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____ (OEM) certifies that, the equipments being sold would not be declared End of Support (EoS) in the next 6 years and that _____ (OEM) shall supply suitable substitute in case EoS of equipments. Also _____ (OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no of years from 6 years to 5 years only for EoS and also from Support point of view. Most of the security solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
29	Additional Points			Solution should provide visibility of all IP addressable devices including IP Phone, IP Camera, IP Printers, IP Scanners etc. - IoT (IP Printer, IP Scanner, IP Phone, IP camera etc) Risk Assessment such as - Detect Insecure (TCP/UDP port open For example IP camera having Telnet Port open etc) - Detect IoT's devices using factory default or Weak/common credentials for SNMP/SSH/TELNET.	Requesting LIC to consider the point since LIC will have ~30% IoT devices which will not support traditional authentication method (such as Radius/DoTIX). It is not a good idea to only depend on 802.1x/MAC address bypass. This is a bad practice since it does not guard against MAC spoofing and other aspects such as hardware changes. Also MAC address repository should be update at any point in time to meet security aspect.	Please refer to the revised "Annexure F"

30	Additional Points			The proposed solution must receive the SIEM data to take policy-based response actions such as quarantining or blocking potentially compromised or noncompliant devices, depending on the severity of the violation information received from SIEM. For example, SIEM detects, via firewall log correlation, a targeted denial of service (DoS) attack. It can direct proposed solution to have the firewall automatically block the source of the attack to prevent further disruption of service to the application(s) on the network.	Garner 2023 Recommendation Enable interoperability with other security solutions. This can be achieved in two ways: customization through open APIs or the use of built-in integration. NAC solutions increasingly feature anomaly detection capability to detect infected endpoints and MAC spoofing attempts on a network. However, integration with other security tools creates a better overall security context for an organization, which can be used to respond automatically to infected endpoints by quarantining them and thus preventing the spread of malware.	Please refer to the revised "Annexure F"
31	Additional Query				Please share total number of Network/L2-L3 devices i.e. Switches, Routers, Access Points, WLC, Firewall etc.	The details shall be shared with the successful bidder
32	Additional Points			Proof of Concept (POC) in Live environment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/ POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response as per timelines signalled from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in their live environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"
33	Section E: Scope of Services	Implementation - point 3 Optimizing & Deployment Validation	52	File tuning of the solutions to be done based on the criteria defined in Technical Specification of each solution and should assure a false positive rate not more than 10% after 1 year for all solutions/services.	Please share the criteria/parameters that will be considered to assure false positive rate not more than 10% after 1 year for all solutions/services	The details shall be shared with the successful bidder, after mutual discussion.
34	Section E: Scope of Services	Training & Certification	54	Training & Certification	Kindly confirm the following - - no of participants for the training - Can the training be done online or it has to be done at onsite at LIC premises?	Please refer to the revised "Section E: Scope of Services"
35	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tools in enterprise environments.	Our understanding is bidder has to leverage OEM PS services to do the end to end implementation. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
36	2. Detailed Scope of Work	I. General Requirements	63	All the solutions should be seamlessly integrated with the LIC's NTP solution and must be compatible with any provided NTP version.	Please confirm which NTP solution is currently used by LIC	The details shall be shared with the successful bidder
37	2. Detailed Scope of Work	I. General Requirements	64	The bidder is required to undertake the migration of historical logs spanning a one-year duration from all existing solutions to new setup. This action is intended to enhance the security posture and to comply with the audit requirements.	Our understanding is the solutions required as part of the RFP are new solutions and there are no existing solution and hence there is no migration that needs to be done. Please confirm	Only the logs of WAF are to be migrated.
38	2. Detailed Scope of Work	III. Network Access Control	65	The vendor must provide the solution that must be compatible with our network infrastructure, supporting integration with our existing switches, routers, and firewalls	Please share the OEM, model and version details of switches, routers and firewall used at LIC	The details shall be shared with the successful bidder
39	5. Resource Deployment	Control SUPPORT REQUIREMENT	85	The Vendor has to construct a portal application with authentication to implement, assess and track various Troubleshooting tickets as well as to post important reports in the web-sites for higher official of LIC. The site has to be updated regularly by the on-site Personnel	Our understanding is bidder needs to propose a TSM tool. If yes, please share the sizing details, technical specifications and sow for the same	Please refer to the revised "Section E: Scope of Services"
40	6. Project Timelines	b. NAC	87	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
41	6. Project Timelines	c. SSL Off loader	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
42	6. Project Timelines	d. WAF	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
43	6. Project Timelines	e. Mobile Device Management	88	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
44	6. Project Timelines	f. API Gateway, Management	89	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	API Gateway and Security Solution has been removed from the scope of this RFP
45	6. Project Timelines	g. Virtual Desktop Interface	89	Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks = D	Request you to consider the delivery timelines as below - - T + 12 weeks = D	Please refer to the revised "Section E: Scope of Services"
46	Key Performance Indicators	Parameter: Backup Frequency	94	Definition: How often data should be backed up to ensure recoverability. Target: Service Level: Daily incremental and Weekly Full Backup	Our understanding is LIC will provide the backup solution to ensure recoverability. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
47	Annexure F	point 2	112	CASB solution should support minimum of 25 users from day 1 with 5 year subscription/license/support and should have flexibility to scale as per future requirements with additional software/subscription license	Page 70 section 3 sizing requirements mentions 1000 roaming users whereas this point mentions 25 users from day 1. Kindly clarify what is the exact count to be considered for sizing and licensing	Please refer to the revised "Annexure F"
48	Annexure C: Eligibility Criteria	point 7	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organizations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request you to amend the clause as below - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 01 (one) organizations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
49	Annexure C: Eligibility Criteria	point 8	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs at least 02 (two) organizations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request you to amend the clause as below - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs at least 01 (one) organizations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
50	Annexure C: Eligibility Criteria	point 9	113	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organizations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Considering this is a new technology that is being adopted by organizations and some of the private firms may not have more than 500 branches. Hence request you to amend the clause as below - The bidder during the last 7 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 01 (one) organizations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
51	Annexure D: Technical Scoring	point 2	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. I Greater than 7 Years -> 10 Marks II Greater than 5 Years up to 7 Years -> 7 Marks III Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder should have relevant implementation and operational experience for 3 out of 7 in scope tools scope tools to PSU/Government/Private/BFSI Sector Firms across different locations in India. I Greater than 7 Years -> 10 Marks II Greater than 5 Years up to 7 Years -> 7 Marks III Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
52	Annexure D: Technical Scoring	point 3	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 2 references of 65000 IP Addresses and above -> 10 Marks II 2 references of 50000 IP Addresses and above -> 7 Marks III 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 2 references of 60000 IP Addresses and above -> 10 Marks II 2 references of 50000 IP Addresses and above -> 7 Marks III 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
53	Annexure D: Technical Scoring	point 4	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 3 references and above -> 10 Marks II 2 references and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 3 references and above -> 10 Marks II 2 references and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
54	Annexure D: Technical Scoring	point 5	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 3 references and above -> 10 Marks II 2 references and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 3 references -> 10 Marks II 2 references and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
55	Annexure D: Technical Scoring	point 6	116	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 2 references of 10000 users and above -> 10 Marks II 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: I 1 reference of 5000 users and above -> 10 Marks II 1 reference of less than 5000 users -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
56	Annexure D: Technical Scoring	point 7	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India I 4 references -> 10 Marks II 2 references -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The bidder/OEM must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India I 4 references -> 10 Marks II 2 references -> 5 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"

57	Annexure D: Technical Scoring	point 8	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India # 4 references -> 5 Marks # 2 references -> 2 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder/OEM must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India # 4 references -> 5 Marks # 2 references -> 2 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
58	Annexure D: Technical Scoring	point 9	116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India # 4 references -> 5 Marks # 2 references -> 2 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you to amend the clause as below - The Bidder/OEM must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India # 4 references -> 5 Marks # 2 references -> 2 Marks (Supporting Document: Bidder (S) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
59	Annexure D: Technical Scoring	point 10	116	The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / ODM Level Certification. Every Additional 5 Resources -> 2 Marks subject to maximum of 10 marks 15 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Request you to amend the clause as below - The bidder must have IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / ODM Level Certification. Every Additional 5 Resources -> 2 Marks subject to maximum of 10 marks 10 Resources -> 5 Marks (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence)	Please refer to the revised "Annexure D"
60	Annexure H: Manufacturer's Authorization Form (MAF)		121	_____(OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6 Years and that _____(OEM) shall supply suitable substitute in case EoS of equipments. Also _____(OEM) certifies that the products being sold would be covered under Warranty / Support and support will be available for next six years (five years initially and one year if extension is provided) from the date of installation at LIC of India.	Requesting LIC to change the no. of years from 6 years to 5 years only for EoS and also from Support point of view. Most of the security solution "appliance" life is not more than 5 years. Hence request you to limit the years to 5 only.	Please refer to the revised "Annexure H"
61	Section C	Annexure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services" and revised "Annexure G"
62	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
63	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should facilitate seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices."	API Gateway and Security Solution has been removed from the scope of this RFP
64	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
65	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
66	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 13	Excel sheet-1	LIC has a heterogeneous network environment comprising of network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	Please let us know that all the network devices in LIC environment are supporting IEEE RADIUS authentication, RADIUS CoA, downloadable ACL, Dynamic ACL and Dynamic VLAN assignment, Multi-Session authentication and multi-domain authentication for policy enforcement on the network device.	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder.
67	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 14	Excel sheet-1	The Solution should be compatible with the existing network environment of the LIC and any future procurement	Please let us know that all the existing network environment in LIC are supporting IEEE RADIUS authentication, RADIUS CoA, downloadable ACL, Dynamic ACL and Dynamic VLAN assignment, Multi-Session authentication and multi-domain authentication for policy enforcement on the network device. Same protocol should be supported in future procurement network device as well.	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder.
68	Annexure F - Technical Compliance	NAC Technical Specification > Point no. 46	Excel sheet-1	The proposed solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma.	Request is to change this clause to The proposed solution should support importing endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma or should support importing of endpoints using XML/API. If Device details information is stored as an XML file, which can be password protected, administrator will enter the same secret key to import the device into the NAC server.	Please refer to the revised "Annexure F"
69	Annexure F - Technical Compliance	NAC Technical Specification	Excel sheet-1	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.)	Please let us know that GDPR compliance or NDPP certification is also applicable for this compliance clause.	Please refer to the revised "Annexure F"
70	2. Detailed Scope of Work	I.General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sitting requirements for NAC, its advised to refer Tech Specs, point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesn't align with this clause. with 50% increase the scalability ask has to be 151000, Request this be clarified so the ambiguity doesn't hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
71	2. Detailed Scope of Work	I.General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
72	2. Detailed Scope of Work	I.General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s) / OEM certified Partner has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
73	2. Detailed Scope of Work	I.General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
74	2. Detailed Scope of Work	I.General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below.	Please refer to the revised "Section E: Scope of Services"
75	2. Detailed Scope of Work	I.General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"
76	2. Detailed Scope of Work	I.General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sitting requirements for NAC, its advised to refer Tech Specs, point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth, the scalability ask should be 263000, Request this be clarified so the ambiguity doesn't hold and also we include the right breakdown of charges for the additional licenses as per this clause	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
77	6. Project Timelines	b.NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 10 Weeks= D	Please refer to the revised "Section E: Scope of Services"
78	Annexure F: Technical Compliance	NAC #67	119	67. The Proposed solution should provide comprehensive visibility of the network by automatically discovering, classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000 devices	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future	The details shall be shared with the successful bidder
79	Annexure F: Technical Compliance	NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDAI, DPDP Act etc)	while we are ISO27001 complied, DPDP act is not fully mature and may take some time to freeze, we request LIC to remove this and also share the IRDAI Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"
80	Annexure F: Technical Compliance	NAC #13	119	13. LIC has a heterogeneous network environment comprising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius CoA standards to support NAC. Request if the Network devices Make and model be shared, we can thoroughly check and appropriately respond.	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder.
81	Annexure F: Technical Compliance	NAC #14	119	The Solution should be compatible with the existing network environment of the LIC and any future procurement	while existing network environ is addressed in #13 of the tech specs, we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius CoA standards	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder.
82	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_____(OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6 Years	Request this be rephrased as below since the declaration of End of support and actual EoS of the product is 2 different interpretations _____(OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6 Years	Please refer to the revised "Annexure H"
83	Compliance			The CASB Solution must have HTTP/2 support from day 1.	This is Web Security (SWG) feature. It is requested to remove this clause.	Please refer to the revised "Annexure F"

84	Compliance			The CASB Solution must have 99% uptime SLA	Considering business applications access via Cloud Service provider,SLA's for Cloud Vendor has to high. Our request to consider 99.999% uptime SLA instead of 99%	Please refer to the revised "Annexure F"
85	Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	This is SWG feature and not CASB feature. CASB is meant to protect SaaS applications and not vulnerabilities.This need SWG license consideration. Kindly relax the point.	Please refer to the revised "Annexure F"
86	Commercial Bid Format				The total value (Column M) does not multiply the price with quantity provided. Kindly request LIC to rectify the commercial format and re-bid.	Please refer to the revised "Annexure G"
87	9. Pricing, Billing, Duties and Taxes	24		c) Prices once fixed will be valid throughout the entire contract period. The Vendor should not, under any circumstances, request for an increase in the prices once prices are approved by LIC. No price variation relating to increases in Government levies/ taxes/ cess/ customs duty & excise duty including any newly introduced taxes shall be permitted.	Taxes, Duties (including Custom Duty), Levies etc are not within bidder's control. Hence the bidder requests LIC to allow for price revision to the extent of revenue in any of these factors by Honourable Government.	Please refer to the revised "Pricing, Billing, Duties and Taxes" and revised "Period of Validity of Bids"
88	25. Placing of Orders and Making Payments	35		a) The Central Office of LIC at Mumbai will place orders (either in full or in phases) with successful bidder for deliverables under this RFP at any time during the validity period of this tender. b) LIC reserves the right to place repeat orders for additional services/ reassessment on the same terms & conditions during the validity of the contract.	The prices are dependent on Taxes, Duties (including Custom Duty), Levies, OEM List Prices, OEM Discounting, USD-INR exchange rate etc. These factors are not within bidder's control and hence we request LIC to allow for price revision on mutually agreeable basis for any subsequent additional order after the 1st PO.	Please refer to the revised "Pricing, Billing, Duties and Taxes" and revised "Period of Validity of Bids"
89	7. Service Level Agreements (SLAs) &	90		Penalty due to delay of 0.2% of total PO value per day.	0.2% of penalty per day is very high value. Kindly request LIC to levy penalty of 0.2% of penalty per week of the undelivered value of materials.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
90	Section G: Payment Terms & Condition	104		The payment terms defined in RFP are as below: o Delivery – 30% o Installation & Integration – 40% o After Go-Live – 25% o Training – 5%	Kindly request LIC to revise the payment terms as below as per industry standards: o Delivery – 70% o Installation & Integration – 20% o After Go-Live – 5% o Training – 5%	Please refer to the revised "Payment Terms & Conditions"
91	Section H: Eligibility Criteria #3	Annexure C: Eligibility Criteria #3	112	The bidder should be in operating-profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 03 (three) out of last 05 (five) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	Considering Bidder's capability to manage the long term sustainability and financial health and manage the Critical network deployment we request LIC to modify clause as below : Bidder should have made profit (before tax) in all the last three financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
92	Section H: Eligibility Criteria #9	Annexure C: Eligibility Criteria #9	112	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02(two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	CASB is a relatively newer technology solution.Request LIC to remove clause as below OR Please modify clause as The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Proxy/ Web Security Gateway/CASB to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
93	Section H: Technical Criteria #2	Annexure D: Technical Criteria #2	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. •Greater than 7 Years -> 10 Marks •Greater than 5 Years up to 7 Years -> 7 Marks •Greater than 3 Years up to 5 Years -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Request LIC to clarify if bidder experience for 3 or 4 out of 7 in scope tools is being evaluated in this criteria for technical scoring.	Please refer to the revised "Annexure D"
94	Section H: Technical Criteria #3	Annexure D: Technical Criteria #3	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: •2 references of 65000 IP Addresses and above -> 10 Marks •2 references of 50000 IP Addresses and above -> 7 Marks •2 references of 25000 IP Addresses and above -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Request LIC to modify clause as below : The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: •2 references of 55000 IP Addresses and above -> 10 Marks •2 references of 40000 IP Addresses and above -> 7 Marks •2 references of 25000 IP Addresses and above -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Please refer to the revised "Annexure D"
95	Section H: Technical Criteria #6	Annexure D: Technical Criteria #6	116	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: •2 references of 10000 users and above -> 10 Marks •2 references of 5000 users and above -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Request you to modify clause as below: The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 1 reference of 20000 users and above -> 10 Marks •1 references of 10000 users and above -> 5 Marks •1 references of 5000 users and above -> 3 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Please refer to the revised "Annexure D"
96	Section H: Technical Criteria #7	Annexure D: Technical Criteria #7	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 50 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •4 references -> 10 Marks •2 references -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 50 APIs in the PSU/Government/Private/BFSI Sector Firms. •2 references and above -> 10 Marks •1 reference -> 5 Marks Atleast one reference should support 1000 Transactions per second. [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Please refer to the revised "Annexure D"
97	Section H: Technical Criteria #8	Annexure D: Technical Criteria #8	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •4 references -> 5 Marks •2 references -> 2 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	CASB is a relatively newer technology solution.Request LIC to remove clause as below OR Please modify clause as The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Proxy/ Web Security Gateway/CASB to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms •2 or More references -> 5 Marks •1 references -> 2 Marks	Please refer to the revised "Annexure D"
98	Section H: Technical Criteria #9	Annexure D: Technical Criteria #9	115	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •4 references -> 5 Marks •2 references -> 2 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India •2 references and above -> 10 Marks •1 reference -> 5 Marks [Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work]	Please refer to the revised "Annexure D"
99	7. Service Level Agreements (SLAs) & Penalties	Annexure F: Service Level Agreements (SLAs) & Penalties	90	Delay in Submission of HLD and LLD beyond 6 weeks from Date of Issue of Purchase order	Request to modify clause: Delay in Submission of HLD and LLD beyond 8 weeks from Date of Issue of Purchase order	Please refer to the revised Service Level Agreements (SLAs) & Penalties
100	7. Service Level Agreements (SLAs) & Penalties	Annexure F: Service Level Agreements (SLAs) & Penalties	90	Penalty is on total deal value	Request to consider penalty as % of delayed deliverable	Please refer to the revised Service Level Agreements (SLAs) & Penalties
101	7. Service Level Agreements (SLAs) & Penalties	Annexure F: Service Level Agreements (SLAs) & Penalties	93	Parameter : Uptime - penalty of 0.25% of total PO value per week of delay or part of thereof	Request to consider penalty as a % of 0.25% of quarterly support value	Please refer to the revised Service Level Agreements (SLAs) & Penalties
102	7. Service Level Agreements (SLAs) & Penalties	Annexure F: Service Level Agreements (SLAs) & Penalties	93 to 96	Penalty is on total deal value	Request Penalty to be aligned to be quarterly invoice value	Please refer to the revised Service Level Agreements (SLAs) & Penalties
103	7. Service Level Agreements (SLAs) & Penalties	Annexure F: Service Level Agreements (SLAs) & Penalties	96	The total penalty for delivery & installation shall not exceed 10% of the PO value	Request penalty to be capped to total value of delayed deliverable.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
104	Section E: Scope of Work	Annexure F: Scope of Work	69	The proposed API Gateway, Management and Security solution should provide real time analytical insights and data.	The Solution can provide user login and session statistics and this can be published to any advanced SIEM for further analysis. Request LIC to confirm this understanding on insights and data.	API Gateway and Security Solution has been removed from the scope of this RFP
105	Annexure F: API Technical Specifications	Annexure F: API Technical Specifications		The solution should achieve and maintain compliance with industry standards, such as PCI DSS, and provide detailed reporting for audit purposes.	Allw understand compliance and encryption to PCI -DSS standards will also be undertaken at the API Creation Activity/End point stage.	API Gateway and Security Solution has been removed from the scope of this RFP
106	Annexure F: API Technical Specifications	Annexure F: API Technical Specifications		The solution should provide automated discovery of backend services and APIs.	We understand this is a feature of WAF solution, hence kindly remove this compliance parameter under API Technical Specifications	API Gateway and Security Solution has been removed from the scope of this RFP
107	Section E: Scope of Work	Annexure F: Scope of Work	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	Request LIC to clarify the Scalability over 5 Year period .	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
108	Section E: Service Level Uptime	Annexure F: Service Level Uptime	92	If the LIC's firewall system uptime for any of the three locations is below 99.9% calculated on monthly basis.	Request LIC to clarify the uptime mention of the "Firewall System" here.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
109	Resource Deployment	Annexure F: Resource Deployment	72	Additional Point Suggested	To maintain operational efficiencies during the contract term and to ensure minimum level of resource quality request LIC to include the following floor limit of resource cost . L1 Resource/Security Analyst- 8 Lacs Per annum L2 Resource/ Security Analysts- 10 Lacs per annum L3 Resource/ Solution Analyst- 15 Lacs Per annum PM - 20 Lacs Per annum	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
110	Section H: 86	Annexure F: 86		The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clause as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
111	2. Detailed Scope of Work	Annexure F: 2. Detailed Scope of Work	68	VII	What are the backend systems with which the API Gateway needs to integrate with? Are there backend systems with published APIs available today within LIC? Can you give a list of systems to be integrated with?	API Gateway and Security Solution has been removed from the scope of this RFP
112	2. Detailed Scope of Work	Annexure F: 2. Detailed Scope of Work	68	VII	Who are the External/Internal users or consumers of the APIs and the API Gateway?	API Gateway and Security Solution has been removed from the scope of this RFP
113	2. Detailed Scope of Work	Annexure F: 2. Detailed Scope of Work	68	VII	How are the APIs being accessed today?	API Gateway and Security Solution has been removed from the scope of this RFP
114	2. Detailed Scope of Work	Annexure F: 2. Detailed Scope of Work	68	VII	Are there plans to monetize APIs? If so, are there any business plans?	API Gateway and Security Solution has been removed from the scope of this RFP
115	2. Detailed Scope of Work	Annexure F: 2. Detailed Scope of Work	68	VII	Is there a requirement for an Internal/external facing Developer Portal for APIs?	API Gateway and Security Solution has been removed from the scope of this RFP

116	2. Detailed Scope of Work	VII. API Gateway, Management and	68	VII	What is the average size of the payload of APIs, in KBs?	API Gateway and Security Solution has been removed from the scope of this RFP
117	2. Detailed Scope of Work	VII. API Gateway, Management and	68	VII	What is the TPS (no. of API calls of an average payload) performance required for the API Gateway?	API Gateway and Security Solution has been removed from the scope of this RFP
118	2. Detailed Scope of Work	VII. API Gateway, Management and	68	VII	What is the average response time required for the API GW?	API Gateway and Security Solution has been removed from the scope of this RFP
119	7. SLAs and Penalties	KPI	95	11	Custom connectors, if required: This clause requires modification. There is no detailed list of backend systems to identify whether custom connectors are required or not. Without that, it is not possible to decide whether custom connectors are required or not.	Please refer to the revised Service Level Agreements (SLAs) & Penalties
120	Annexure F - Technical Compliance	NAC Technical Specification	Excel sheet-1		The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as IRDAI, DPDP Act etc.) Please let us know that GDPR compliance or NDPP certification is also applicable for this compliance clause.	Please refer to the revised "Annexure F"
121	Section G	Clause 1	104		Payment Terms & Conditions Bidder request to change the milestone as below 1. 70% on delivery of SW 2. 20% on installation and integration 3. 5% on FAT 4. 5% on completion of training	Please refer to the revised "Payment Terms & Conditions"
122	24	g	34		The PBG may be invoked for entire amount if the vendor backs-out of his obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG, apart from other actions that may be decided by LIC. We request that the clause be deleted and replaced as below: "Subject to a notice and cure period of not less than 30 days, the PBG may be invoked solely for material breaches of the Contract."	The PBG may be invoked for entire amount, after providing a cure period of 30 days in writing, if the vendor backs-out of its obligations as per this tender or if the fresh PBG is not received by LIC one month prior to the expiry of the earlier PBG, apart from other actions that may be decided by LIC.
123	27	a	35		Bids shall remain valid for 12 months from the last date of bid submission as prescribed by LIC, in the Activity Schedule. We would kindly request that this duration be shortened to 3 months, as it becomes difficult to keep all the price rates for the same services fixed for a longer duration.	Please refer to the revised "Period of Validity of Bids"
124	27	f	36		The commercial offer shall be on a fixed price basis for the contract period. No upward revision in the price would be considered on account of subsequent increases during the offer validity period except for GST and any other applicable taxes. We would request that this clause be deleted as it becomes difficult to account for all potential change in prices (both upward and downward) for the entire duration of 60 months, i.e. 5 years, owing to several factors out of our hands.	Please refer to the revised "Period of Validity of Bids"
125	Section E	1	53		The SI shall have to comply with LIC's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the finally selected Bidder. We kindly request that this policy be shared with us beforehand so that we can ensure compliance with the same.	The details shall be shared with the successful bidder
126	8		101		Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract. We would request that the clause be amended as follows: "Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract, after a cure period of 30 days and notice have been provided."	Notwithstanding what has been stated in this RFP LIC may, without prejudice to any other remedy for breach of contract, by written notice of default sent to the Vendor, terminate the Contract in whole or part if the Vendor fails to deliver any or all of the systems within the period(s) specified in Scope of Work of the RFP, or if the Vendor fails to perform any other obligation(s) under the Contract after a cure period of 30 days have been provided in writing.
127	Annexure C: Eligibility Criteria	5	112		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organisations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP Can the IP count or branches count be reduced?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
128	Annexure C: Eligibility Criteria	6	112		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. Can we submit single experience details? Can you amend the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
129	Annexure C: Eligibility Criteria	8	113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. Can this be revised to 1 organisations with the amendment in the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
130	Annexure C: Eligibility Criteria	9	113		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. Can this be revised to 1 organisations with the amendment in the branches count as well?	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
131	Annexure C: Eligibility Criteria	11	113		The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably of the proposed OEM). Please amend the count to minimum 5 resources	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
132	G	Section G: Payment Terms &	104		Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. Please amend this to 100% after delivery of software licenses along with invoice	Please refer to the revised "Payment Terms & Conditions"
133	G	Section G: Payment Terms &	104		Installation and integration, initial OEM audit and acceptance testing as per scope of work. Please amend this to 50% advance and balance 50% on completion	Please refer to the revised "Payment Terms & Conditions"
134	Annexure F - Technical Compliance VDI Pointers_	40	NA		The solution should be able to encrypt end to end traffic from end user to network to controller/broker Since Broker remains in LAN and connect VDI server in LAN only, the encryption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able to encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
135	Annexure F - Technical Compliance VDI Pointers_	49	NA		The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders Expectation in line is not clear, request to add specific requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
136	Annexure F - Technical Compliance VDI Pointers_	66	NA		The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable. In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent advancement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool Audio & Video. Also Flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
137	Annexure F - Technical Compliance VDI Pointers_	73	NA		The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
138	Annexure F - Technical Compliance VDI Pointers_	76	NA		The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment. launch time of VDI depends on many factors, like AD, Group policy, printer and drive mapping it requires more times than default desktop, 5 second login time is unachievable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
139	Annexure C: Eligibility criteria	Page 113/Sr.No. 8			The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India. The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
140	Section G - Payment Terms &	Page 104			Point No 3 - Payment schedule table As we will be supplying perpetual license at the beginning, 100% license cost should be paid once licenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
141	2. Detailed Scope of Work	I. General Requirements	63		The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications. In the sizing requirements for NAC, it's advised to refer Tech Spec, point 67 towch mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000. Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
142	2. Detailed Scope of Work	I. General Requirements	63		The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments. Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments	Please refer to the revised "Section E: Scope of Services"
143	2. Detailed Scope of Work	I. General Requirements	63		The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project. Request this be modified as below The bidder shall ensure that the OEM(s) / OEM certified Partner has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
144	2. Detailed Scope of Work	I. General Requirements	63		The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM. Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
145	2. Detailed Scope of Work	I. General Requirements	63		The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below: Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
146	2. Detailed Scope of Work	I. General Requirements	63		The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise. Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"

147	2. Detailed Scope of Work	I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sitting requirements for NAC, it's advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000. Request this be clarified so the ambiguity doesn't hold and also we include the right breakdown of charges for the additional licenses as per this clause	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
148	4. RACI Matrix	2. Network Access Control	71	Software Implementation - OEM - A-C	Request this be changes as below Software Implementation - OEM - C	Please refer to the revised "Section E: Scope of Services"
149	4. RACI Matrix	2. Network Access Control	71	SLA Performance -OEM- C	Request this be changes as below SLA Performance -OEM- C	Please refer to the revised "Section E: Scope of Services"
150	6. Project Timelines	b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. => T + 5 Weeks D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. => T + 10 Weeks D	Please refer to the revised "Section E: Scope of Services"
151	Annexure F - Technical Compliance	NAC #13	119	13. LIC has a heterogeneous network environment comprising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC. Request if the Network devices Make and model be shared , we can thoroughly check and appropriately respond.	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
152	Annexure F - Technical Compliance	NAC #14	119	The solution should be compatible with the existing network environment of the LIC and any future procurement in future to have support for IEEE 802.1x and Radius COA standards	while existing network environment is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
153	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_(OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _(OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
154	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
155	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting points, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should facilitate seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices."	API Gateway and Security Solution has been removed from the scope of this RFP
156	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
157	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by Blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
158	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	3	Device should be based on dedicated -xU hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40 vCPUs scalable to 60 vCPUs.	Query: - RFP has asked for Less than 2RU i.e. 1RU form factor for Proposed appliance, which is not true for all OEM, i.e. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size of CPU which changes the need of number of vCPUs and cannot be binding factor and due to this request to relax the specs Hence we request to relax the requirement to below Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
159	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	4	Should have minimum SSL visibility throughput of 146 Gbps from day 1 and scalable to 195 Gbps on same platform with hardware compression.	Suggestion: for the SSLio like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill Hence request to change the specs to below: Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F"
160	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	5	Should support minimum SSL Visibility TPS: -260 K TPS (RSA 2k keys) from day 1 and scalable to 400 K TPS (RSA 2k keys) on same platform - 180 K TPS (ECDHE-ECDSA P-256) from day 1 and scalable to 300 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM Hence request to change the specs to below: Should support minimum SSL Visibility TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform -70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please refer to the revised "Annexure F"
161	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	7	The proposed solution should have a 45 Gbps bulk encryption from Day 1 and scalable to 100 Gbps bulk encryption	Suggestion: Having such high SSL throughput for 100Gbps seems to be overkill Hence request to change the specs to below: The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F"
162	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appliance due to unpredictable traffic flow and increases troubleshooting complexity Hence request to change the specs to below The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
163	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	18	The solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM Hence request to change the specs to below The solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"
164	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows through existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLIO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust applications access with SAML/Oauth with MFA and Secure web gateway (explicitly proxy) functionality with add-on licenses if required in future	Query: - The features asked in the specs seems to be specific to particular OEM and below technology seems not to be related to SSLio Solution - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicitly proxy) functionality Hence request to change the specs to below SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows through existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLIO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
165	Annexure F - Technical Compliance	SSL Offloader Tech Specs	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-In-The-Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
166	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	81	The SSL Offloader device should be able to have flexible ICAP request or respond policies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bin", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/javascript)	This is specific to a single OEM, hence request to change the specs to below The SSL Offloader device should be able to have flexible ICAP request or respond policies.	Please refer to the revised "Annexure F"
167	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	3	Device should be based on dedicated 1U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24 vCPUs scalable to 36 vCPUs.	Query: - RFP has asked for Less than 2RU i.e. 1RU form factor for Proposed appliance, which is not true for all OEM, i.e. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size of CPU which changes the need of number of vCPUs and cannot be binding factor and due to this request to relax the specs Hence we request to relax the requirement to below Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not	Please refer to the revised "Annexure F"
168	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	4	Should have minimum SSL visibility throughput of 115 Gbps from day 1 and scalable to 175 Gbps on same platform with hardware compression.	Suggestion: for the SSLio like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill Hence request to change the specs to below: Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities .	Please refer to the revised "Annexure F"
169	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	5	Should support minimum SSL Visibility TPS: -100 K TPS (RSA 2k keys) from day 1 and scalable to 180 K TPS (RSA 2k keys) on same platform - 75 K TPS (ECDHE-ECDSA P-256) from day 1 and scalable to 125 K TPS (ECDHE-ECDSA P-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM Hence request to change the specs to below: Should support minimum SSL Visibility TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform -70 K TPS (ECDHE-ECDSA P-256) from day 1 on same platform	Please refer to the revised "Annexure F"

170	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appliance due to unpredictable traffic flow and increases troubleshooting complexity Hence request to change the specs to below The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
171	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	18	The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM Hence request to change the specs to below The Solution must support both Inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption	Please refer to the revised "Annexure F"
172	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/ OAuth with MFA and Secure web gateway (explicitly proxy) functionality with add-on licenses if required in future	Query: The features asked in the specs seems to be specific to particular OEM and below technology seems not to be related to SSLO Solution - Zero trust application access with SAML/ OAuth with MFA - Secure web gateway (explicitly proxy) functionality Hence request to change the specs to below SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSLO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
173	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-In-The-Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
174	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	81	The SSL Offloader device should be able to have flexible ICAP request or respond policies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	This is specific to a single OEM, hence request to change the specs to below The SSL Offloader device should be able to have flexible ICAP request or respond policies.	Please refer to the revised "Annexure F"
175	6 Eligibility Criteria	Sr. No. 4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 2 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
176	6 Eligibility Criteria	Sr. No. 5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP	We request to revise the criteria as below: "The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
177	6 Eligibility Criteria	Sr. No. 6	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
178	6 Eligibility Criteria	Sr. No. 7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
179	6 Eligibility Criteria	Sr. No. 8	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 01 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
180	6 Eligibility Criteria	Sr. No. 9	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We request to revise the criteria as below: "The bidder / OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India."	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
181	24 Performance Bank Guarantee	a)	34	After finalisation of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having branches in Mumbai) equal to 10% of the Total Contract Value.	As per the revised Rule 17(1)(i) of GFR 2017, the performance security should be for an amount of 3 to 10% of contract value. Therefore, we request you to reduce this Performance Bank Guarantee to 5% of the Total Contract Value.	After finalisation of the RFP process, the selected bidder should submit an unconditional and irrevocable Performance Bank Guarantee (from a scheduled/ nationalized Public Sector Bank acceptable to LIC and having branches in Mumbai) equal to 5% of the Total Contract Value.
182	Section G:	Sr. No. 1	104	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC - 30% of Cost	We request to revise the payment clause as below: "Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC - 70% of Cost"	Please refer to the revised "Section E: Scope of Services"
183	Section G:	Sr. No. 2	104	Installation and integration, initial OEM audit and acceptance testing as per scope of work - 40% Of Cost	We request to revise the payment clause as below: "Installation and integration, initial OEM audit and acceptance testing as per scope of work - 20% Of Cost"	Please refer to the revised "Section E: Scope of Services"
184	Section G:	Sr. No. 3	104	After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 25% of Cost	We request to revise the payment clause as below: "After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 5% of Cost"	Please refer to the revised "Section E: Scope of Services"
185	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC, its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000, Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services" and revised "Annexure F"
186	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEM/s / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
187	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s) / OEM certified Partner has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
188	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
189	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
190	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"
191	Section E: Scope of Services	2. Detailed Scope of Work I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sizing requirements for NAC, its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000, Request this be clarified so the ambiguity doesnt hold and also we include the right breakdown of charges for the additional licenses as ked in this clause	Please refer to the revised "Section E: Scope of Services"
192	Section E: Scope of Services	4. RACI Matrix	71	2. Network Access Control (NAC) Software Implementation - OEM - A-C	Request this be changes as below Software Implementation - OEM - C	Please refer to the revised "Section E: Scope of Services"
193	Section E: Scope of Services	4. RACI Matrix	71	2. Network Access Control (NAC) SLA Performance - OEM - C	Request this be changes as below SLA Performance - OEM - C	Please refer to the revised "Section E: Scope of Services"
194	Section E: Scope of Services	6. Project Timelines b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks= D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 10 Weeks= D	Please refer to the revised "Section E: Scope of Services"
195	Section H: Enclosures	Annexure F: Technical Compliance NAC #13	119	13. LIC has a heterogeneous network environment comprising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC. Request if the Network Devices Make and model be shared , we can thoroughly check and appropriately respond.	Network Devices in LIC's Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
196	Section H: Enclosures	Annexure F: Technical Compliance NAC #14	119	14. The Solution should be compatible with the existing network environment of the LIC and any future procurement in future to have support for IEEE 802.1x and Radius COA standards.	while existing network enviroint is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards.	Network Devices in LIC's Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
197	Section H: Enclosures	Annexure F: Technical Compliance NAC #67	119	67. The Proposed solution should provide comprehensive visibility of the network by automatically discovering , classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000 devices	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future.	The details shall be shared with the successful bidder
198	Section H: Enclosures	Annexure F: Technical Compliance NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDA, DPSP Act etc)	while we are ISO27001 complied, DPSP act is not fully mature and may take some time to freeze, we request LIC to review this and also share the IRDA Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"

199	Section H: Enclosures	Annexure H: Manufacturer's Authorization Form	121	_(OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6 Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _(OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
200	Queries for Eligibility Criteria	Section B) Eligibility no- 4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We are requesting for... The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms within different Locations across in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
201	Section B) 6 Eligibility Criteria Point no.5	Section B) Eligibility Criteria No.5 to no.9	14,15	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	LIC has asked for Four- in-scope Solutions out of 7, in E Criteria no.4, & from criteria No.5 to Criteria no.9 you have asked for 5 individual in scope solutions (No.5# NAC, No.6# WAF, No.7 # MDM/SSLO, No.8 #VDI/API Gateway, No.9# CASB). These are 5- individual solutions, Kindly confirm on 4 out of 7.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
202	Section B) 6 Eligibility Criteria Point 9)	Section B) Eligibility Criteria No.9	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We are requesting to remove this Criteria, for bidder. (please keep it for Proposed OEM)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
203	Section B) Eligibility Criteria No.5	Section B) Eligibility Criteria No.5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different Locations in India	We are Proposing For:- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least One organisations in PSU/Government/Private/BFSI Sector Firms across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
204	Section B) Eligibility Criteria No.6	Section B) Eligibility Criteria No.6	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
205	Section B) Eligibility Criteria No.7	Section B) Eligibility Criteria No.7	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	WE ARE PROPOSING FOR:- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least ONE organisations in PSU / Government / Private / BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
206	Section B) Eligibility Criteria No.8	Section B) Eligibility Criteria No.8	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	WE ARE PROPOSING FOR :- The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least One organisations in PSU / Government / Private / BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
207	Annexure F - Technical Compliance VDI Pointers_		40	NA	The solution should be able to encrypt end to end traffic from end user to network to controller/broker Since Broker remains in LAN and connect VDI server in LAN only, the encryption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able to encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
208	Annexure F - Technical Compliance VDI Pointers_		49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders Expectation in line is not clear, request to add sepecic requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"
209	Annexure F - Technical Compliance VDI Pointers_		66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent achievement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool Audio & Video. Also Flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable.	Please refer to the revised "Annexure F"
210	Annexure F - Technical Compliance VDI Pointers_		73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
211	Annexure F - Technical Compliance VDI Pointers_		76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment. Launch time of VDI depends on many factors, like AD, Group policy, printer and drive mapping it requires more times than default desktop, 5 second login time is unachievable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
212	Annexure C - Eligibility criteria	Page 113/Sr.No.8		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
213	Section G - Payment Terms &	Page 104		Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once licenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
214	6	4	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The Bidder should have minimum of 2 years of experience in Implementing or supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
215	6	5	14	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have implemented or supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
216	6	15	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
217	7	15	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 01 (one) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
218	8	15	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder / oem during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 01 (one) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
219	9	15	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify to - The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 01 (one) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Customer do buy directly and prefer SI for implement / support. Request to modify the same.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
220	Scope of Work		55	Support Process Requirement The vendor has to create separate interfaces for them/LIC administrators to carry out the minimum possible jobs, which may be changed as per the business needs ensuring compliance to LIC security policies. There should be a provision to audit the changes done to fix the accountability.	Need clarity on the separate interface requirements. Is bidder expected to provide any tool for Incident or Change management?	Please refer to the revised "Section E: Scope of Services"
221	Scope of Work		56	The Vendor has to provide a portal application with authentication to implement, assess and track various trouble-tickets to higher officials of LIC. The site has to be updated regularly by the on-site Personnel	Is Bidder expected to provide any ITSM tool? If not, need clarity on expectations from bidder. Need clarity on portal application mentioned in the statement.	Please refer to the revised "Section E: Scope of Services"
222	Scope of Work		56	No telephone connection will be provided by LIC to the onsite support persons	We assume here telephone connection refers to mobile phone for the onsite resources. Kindly confirm. We assume other logistics like seating space, desktop and other admin facilities would be provided by LIC to the	Logistics like seating space, desktop and other admin facilities would be provided by LIC to the onsite resources
223	Onsite-support Services	NAC	58	For initial phase 24x7 number of onsite support is required later after the solution is implemented and stable the number of onsite resources for monitoring would be 8x5.	What is the expected timeline for 24*7? Can we assume 8*5 support 2nd year onward?	Please refer to the revised "Section E: Scope of Services"
224	3. Sizing Requirements	All Solutions	70	Sizing Parameters	1. Is HA required to be factored for all solutions? Please confirm. 2. What all solution among the list shared are new addition or replacement of the existing technologies?	Please refer to the revised "Section E: Scope of Services"
225	5. Resource Deployment	Project Coordinator	73	Project Coordinator - count 1	1. Is Project coordinator required to be onsite? 2. What is the expected coverage windows?	Please refer to the revised "Section E: Scope of Services"
226	5. Resource Deployment	CASB	73	CASB - The L1 resource shall be utilized in a shared mode from the network resource deployment.	Need clarity how to leverage shared resource. What is "Network Resource Deployment"?	Please refer to the revised "Section E: Scope of Services"
227	5. Resource Deployment	NAC SSLO WAF MDM	73-77	L1 and L2 Resource Count - 24*7 Coverage	We understand for each mentioned technology solution bidder to provision 2*L2 and 2*L1 Resources i.e 4 per technology to provide 24*7 onsite support coverage. Kindly confirm if the understanding is correct.	Please refer to the revised "Section E: Scope of Services"
228	5. Resource Deployment	API VDI	78-80	L1 and L2 Resource - Solution Analyst	Kindly confirm the support coverage. Is it 8*5 support from LIC office?	Please refer to the revised "Section E: Scope of Services"
229	Onsite Support Services	SUPPORT PROCESS REQUIREMENT	85	Day-to-day maintenance of the network gateway security setup along with associated appliances like routers, switches, Link load balancers etc. which may be provided by LIC.	Need Clarity on Other components to be managed by Bidder's team. Request LIC team to provide list of components along with the scope.	Please refer to the revised "Section E: Scope of Services"
230	Onsite Support Services	Remote (offsite) Support	86	Remote (offsite) Support	Request LIC to confirm following on Remote Support Ask: 1. Remote Support Coverage Window? 2. Number of Resources per technology for remote support 3. Scope of Remote Support Team for each technology	Please refer to the revised "Section E: Scope of Services"
231	Onsite Support Services	Service-Delivery and Project Management	86	The selected vendor will have to post a full-time onsite Service-Delivery Manager (SDM) immediately after the signing of the Contract.	Is Project coordinator and Service Delivery manager Same or Bidder need to factor separate Project coordinator and Service Delivery Manager?	Please refer to the revised "Section E: Scope of Services"

232	3. Sizing Requirements	All Solutions	70	Sizing Parameters	1. Reuqets LIC to share the Application inventory to be onboarded on WAF/API 2. Reuqets LIC to share the one time implementation scope for each technology	Please refer to the revised "Section E: Scope of Services"
233	Section C	Annexure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services"
234	Section H	Annexure F, 10		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS, TACACS+ or via local table of authorized users.	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS/TACACS+ /via local table of authorized users."	Please refer to the revised "Annexure F"
235	Section H	Annexure F, 86		The solution must protect system against WASC Wec Security Attack classification.	Request to modify the clause as "The solution must protect system against WASC Wec Security Attack classification or OWASP top 10."	Please refer to the revised "Annexure F"
236		Compliance			The CASB Solution must have HTTR/2 support from day 1.	Please refer to the revised "Annexure F"
237		Compliance			The CASB Solution must have 99% uptime SLA	Please refer to the revised "Annexure F"
238		Compliance			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats	Please refer to the revised "Annexure F"
239	Annexure F - Technical Compliance	API GW	13	The solution should provide features to Convert between different data formats (e.g., JSON to XML).	We request LIC to reconsider older protocol supports like XML is an outdated API protocol, also JSON to XML translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The solution should provide seamless integration with additional package to Convert between different data formats (e.g., JSON to XML) without adding overheads API-GW solution."	API Gateway and Security Solution has been removed from the scope of this RFP
240	Annexure F - Technical Compliance	API GW	19	The proposed solution should facilitate seamless SOAP to REST transformation, enabling interoperability by translating SOAP-based requests into RESTful API calls, promoting modern integration practices.	We request LIC to reconsider older protocol supports like SOAP is XML based outdated API protocol, also SOAP (XML) to REST (JSON) translation will introduce good amount of latency and in future, it will introduce more troubleshooting point, which requires high skill to understand and resolve. We hereby request LIC to kindly change this point as: "The proposed solution should seamless integration with additional package to translate SOAP to REST, enabling interoperability by translating SOAP-based requests into RESTful API calls as and when required without adding overheads API-GW solution, promoting modern integration practices".	API Gateway and Security Solution has been removed from the scope of this RFP
241	Annexure F - Technical Compliance	API GW	20	The solution should be designed to facilitate a developer organization by providing comprehensive tools, documentation, and support for efficient development.	We request LIC to consider that the mentioned features are getting fulfilled with development tools, not by API gateway, introducing it on API GW will increase overhead and it force developer to restrict themselves to limited features available on such tool. We request LIC to change this clause as: "The solution should be designed to facilitate to integrate it with developer organization by providing compatibility with multiple tools and support for efficient development with the Security of authentication, authorization, payload sanitization and WAF signature inspection"	API Gateway and Security Solution has been removed from the scope of this RFP
242	Annexure F - Technical Compliance	API GW	31	The API gateway should implement streaming APIs using compatible protocols like WebSocket, WebSub, or server-sent events.	We request LIC to kindly change this clause as webSub is a protocol usually used to push content by many websites, including all blogs served by blogger and WordPress.com news sites. This use case seems to be irrelevant to LIC. Recommended revised clause: "The API gateway should implement streaming APIs using compatible protocols like WebSocket and server-sent events and support WebSub via plugins/packages."	API Gateway and Security Solution has been removed from the scope of this RFP
243	2. Detailed Scope of Work	I. General Requirements	63	The services and solutions provided should possess modularity and scalability to effectively meet the LIC's needs throughout the five-year contract period. Over the 5-year contract period, bidder may consider an increase of 50% in the number of devices or solutions to be monitored when determining system specifications.	In the sizing requirements for NAC, its advised to refer Tech Specs , point 67 towich mentions "Total of 127000 endpoint devices and scalable to 160000 devices" above is only 26% and doesnt align with this clause. with 50% increase the scalability ask has to be 191000. Request this be clarified so the ambiguity doesnt hold	Please refer to the revised "Section E: Scope of Services"
244	2. Detailed Scope of Work	I. General Requirements	63	The bidder / System Integrator shall engage the services of respective OEMs for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Request this be modified as below The bidder / System Integrator shall engage the services of respective OEMs / OEM certified Partner for plan, design, and implementation of the solution. The OEM(s) must deploy subject matter experts with experience in designing and implementation of the respective tool in enterprise environments.	Please refer to the revised "Section E: Scope of Services"
245	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the OEM(s) has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Request this be modified as below The bidder shall ensure that the OEM(s) OEM certified Partner has end to end responsibility for plan, design, implementation, maintenance, and adoption of the total solution leveraging the behavior modeling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.	Please refer to the revised "Section E: Scope of Services"
246	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM.	Request this be modified as below The bidder shall ensure that the configuration, implementation, and testing of the solution components to be carried out by resources from the OEM / OEM certified Partner as decided by LIC at the time of implementation. The bidder's resources can be leveraged; however, the overall responsibility of the implementation shall be with OEM / OEMs certified Partner.	Please refer to the revised "Section E: Scope of Services"
247	2. Detailed Scope of Work	I. General Requirements	63	The bidder shall also engage the services of the respective OEMs for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Request this be modified as below The bidder shall also engage the services of the respective OEMs / OEMs Certified Partner for post implementation audit, validation, and certification by the OEM that the solution has been implemented as per the plan & design provided by them.	Please refer to the revised "Section E: Scope of Services"
248	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Request this be modified as below The bidder and OEM / OEMs certified Partner services team shall conduct a workshop with all the departments of LIC to gather the inputs in relation to solution requirement with respect to the baselining and scoping of the components including the items listed below:	Please refer to the revised "Section E: Scope of Services"
249	2. Detailed Scope of Work	I. General Requirements	63	The bidder and OEM services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Request this be modified as below The bidder and OEM/OEM certified Partner services team shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.	Please refer to the revised "Section E: Scope of Services"
250	2. Detailed Scope of Work	I. General Requirements	64	The vendor should arrange for a comprehensive deployment audit done by OEM after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Request this be changed as The vendor should arrange for a comprehensive deployment audit done by OEM / OEMs certified partner after completion of initial deployment and at the end of the first and second year of initial deployment. The audit would be base lined against SOW, deliverables, LIC Policies and industry best practices. This would be linked to the payment against installation.	Please refer to the revised "Section E: Scope of Services"
251	2. Detailed Scope of Work	I. General Requirements	64	All solutions must have the capacity to accommodate a yearly project growth rate of up to 20%. The upfront quotation for all licenses should be transparent and also include a breakdown of charges for additional licenses, considering the anticipated 20% YoY project growth.	In the sizing requirements for NAC, its advised to refer Tech Specs , point 67 to which mentions "Total of 127000 endpoint devices and scalable to 160000 devices" With 20% YoY growth , the scalability ask should be 263000. Request this be clarified so the ambiguity doesnt hold and also we include the right breakdown of charges for the additional licenses as ked in this clause	Please refer to the revised "Section E: Scope of Services"
252	4. RACI Matrix	2. Network Access Control	71	Software Implementation - OEM - A-C	Request this be changes as below Software Implementation - OEM - C	Please refer to the revised "Section E: Scope of Services"
253	4. RACI Matrix	2. Network Access Control	71	SLA Performance - OEM - C	Request this be changes as below SLA Performance - OEM - C	Please refer to the revised "Section E: Scope of Services"
254	6. Project Timelines	b. NAC	87	2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 5 Weeks- D	Request this be changed to below 2. Delivery of all the equipment as quoted in the bill of materials for each solution in-scope. Date of delivery of last item shall be taken as date of delivery for all items. - T + 10 Weeks- D	Please refer to the revised "Section E: Scope of Services"
255	Section G: Payment Terms & Conditions		104	Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - 30% Installation and integration, initial OEM audit and acceptance testing as per scope of work- 40% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 25% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work. - 5%	Request to change as follows - Delivery of software and appliances (if any) at all designated sites of LIC for the project and signing of the contract with LIC. - 50% Installation and integration, initial OEM audit and acceptance testing as per scope of work- 30% After Go Live i.e., after acceptance test and audit, validation and certification by all the respective OEM/s - 15% Training/knowledge transfer, documentation of entire solution at specified locations as per the scope of work. - 5%	Please refer to the revised "Section E: Scope of Services"
256	Annexure F: Technical Compliance	NAC #67	119	67. The Proposed solution should provide comprehensive visibility of the network by automatically discovering , classifying and enforcing policy for endpoints connected to the network and must have capacity to support the appropriate service for a total of 127000 endpoint devices and scalable to 160000 devices	Request the count of end user devices and the headless devices be please shared out of the asked 127000 now and 160000 devices in future	The details shall be shared with the successful bidder
257	Annexure F: Technical Compliance	NAC #69	119	69. The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001 etc) and any applicable Laws and regulations (such as IRDAI, DPDP Act etc)	while we are ISO27001 complied , DPDP act is not fully mature and may take some time to freeze, we request LIC to remove this and also share the IRDAI Laws and regulations Document to check for compliance	Please refer to the revised "Annexure F"
258	Annexure F: Technical Compliance	NAC #13	119	13. LIC has a heterogeneous network environment comprising network devices of various OEM and models. The proposed solution should support all the network make and model devices without requesting LIC for any changes in terms of any hardware and software	The Network devices should support IEEE 802.1x and Radius COA standards to support NAC. Request if the Network devices Make and model be shared , we can thoroughly check and appropriately respond.	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
259	Annexure F: Technical Compliance	NAC #14	119	The Solution should be compatible with the existing network environment of the LIC and any future procurement	while existing network enviroint is addressed in #13 of the tech specs , we request LIC to procure any routers/switches in future to have support for IEEE 802.1x and Radius COA standards	Network Devices in LICs Network are managed devices from different OEMs. The complete details shall be provided to the successful bidder .
260	Annexure H: Manufacturer's Authorization Form (MAF)	N/A	121	_(OEM) certify that, the equipments being sold would not be declared End of Support (EoS) in the next 6Years	Request this be rephrased as below since the declaration of End of support and actual EOS of the product is 2 different interpretations _(OEM) certify that, the equipments being sold would not be End of Support (EoS) in the next 6Years	Please refer to the revised "Annexure H"
261	Annexure F - Technical Compliance VDI Printers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encryption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
262	Annexure F - Technical Compliance VDI Printers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecic requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"

263	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent advancement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool's Audio & Video. Also Flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
264	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
265	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	Launch time of VDI depends on many factors, like AD, Group policy, printer and drive mapping it requires more times than default desktop, 5 second login time is unachievable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
266	Annexure C - Eligibility criteria	Page 113/Sr.No 8		The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
267	Eligibility Criteria	Eligibility Criteria	14	5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organisations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	As multiple Pre-qualification criteria over another is narrowing participation. Hence, we request LIC to consider below clause. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 15,000 IP Addresses to at least 01 (two) organisations in PSU/Government/Private/BFSI Sector Firms. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organisations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
268	Eligibility Criteria	Eligibility Criteria	14	6. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to remove restriction of 500 Branches as it may not be relevantly applicable to PSU/Government 6. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
269	Eligibility Criteria	Eligibility Criteria	14	7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	As multiple Pre-qualification criteria over another is narrowing participation. Hence, we request LIC to consider below clause. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 01 (two) organisations in PSU / Government / Private / BFSI Sector Firms.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
270	Eligibility Criteria	Eligibility Criteria	14	8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Request LIC to consider below clause 8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Protection & Discovery - Access Control/ API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
271	Eligibility Criteria	Eligibility Criteria	14	9. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to consider below clause 9. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB)/DLP to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
272	Eligibility Criteria	Eligibility Criteria	14	The bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request LIC to change "The Bidder should have minimum of 3 years of experience in supplying, implementing, or supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
273	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. # Greater than 7 years -> 10 Marks # Greater than 5 years up to 7 years -> 7 Marks # Greater than 3 years up to 5 years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms # Greater than 7 years -> 10 Marks # Greater than 5 years up to 7 years -> 7 Marks # Greater than 3 years up to 5 years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
274	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	115	3. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 2 references of 65000 IP Addresses and above -> 10 Marks # 2 references of 50000 IP Addresses and above -> 7 Marks # 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause 3. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 2 references of 15000 IP Addresses and above -> 10 Marks # 2 references of 10000 IP Addresses and above -> 7 Marks # 2 references of 5000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
275	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	115	4. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 3 references and above -> 10 Marks # 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause 4. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: - 3 references and above -> 10 Marks - 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
276	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	115	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 3 references and above -> 10 Marks 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader/NGFW/Webproxy solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 3 references and above -> 10 Marks 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
277	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	Annexure D: Technical Scoring Technical Evaluation Criteria - Parameters	115	6. The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 2 references of 10000 users and above -> 10 Marks # 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request you LIC to consider below technical scoring clause 6 The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: # 2 references of 5000 users and above -> 10 Marks # 2 references of 3000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
278	Annexure F - Technical Compliance VDI Pointers_	40	NA	The solution should be able encrypt end to end traffic from end user to network to controller/broker	Since Broker remains in LAN and connect VDI server in LAN only, the encryption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
279	Annexure F - Technical Compliance VDI Pointers_	49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders	Expectation in line is not clear, request to add sepecic requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders	Please refer to the revised "Annexure F"

280	Annexure F - Technical Compliance VDI Pointers_	66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable	In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent advancement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool's Audio & Video. Also flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
281	Annexure F - Technical Compliance VDI Pointers_	73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing	HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
282	Annexure F - Technical Compliance VDI Pointers_	76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment.	Launch time of VDI depends on many factors, like AD, Group policy, printer and drive mapping it requires more times than default desktop, 5 second login time is unachievable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
283	Annexure C - Eligibility Criteria	Page 113/5	8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
284	Section G - Payment Terms & Conditions	Page 104	Point No 3 - Payment schedule table		As we will be supplying perpetual license at the beginning, 100% license cost should be paid once licenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
285	Eligibility Criteria				LIC To accept 100% owned subsidiary experience & work orders	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
286	Annexure C - Eligibility Criteria	112		The bidder should be in operating profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 03 (three) out of last 05 (five) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	The bidder should be in operating profit (EBITDA i.e., Earnings before Interest, Tax, Depreciation & Amortization) during the last 03 (three) years preceding the date of this RFP or The bidder should have made profit (before tax) in any of the 02 (two) out of last 03 (three) financial years preceding the date of this RFP and should be having positive net worth for the last 03 (three) financial years preceding to the date of this RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
287	Annexure C - Eligibility Criteria	112		4. The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 4. The Bidder or bidder's parent company (incase bidder is wholly owned subsidiary of its parent company) should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
288	Annexure C - Eligibility Criteria	112		5. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 5. The bidder or BIDDER'S PARENT COMPANY during the last 7 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
289	Annexure C - Eligibility Criteria	112		6. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 6. The bidder or BIDDER'S PARENT COMPANY during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
290	Annexure C - Eligibility Criteria	112		7. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 7. The bidder or BIDDER'S PARENT COMPANY during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
291	Annexure C - Eligibility Criteria	112		8. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Request to modify the clause as: 8. The bidder or BIDDER'S PARENT COMPANY/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
292	Annexure C - Eligibility Criteria	112		9. The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	9. The bidder /OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
293	Annexure C - Eligibility Criteria	112		10. The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / ODM Level Certification. Minimum 3 resources must have ODM Level Certification (preferably any or combination of the proposed OEM).	10. The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / ODM Level Certification. Minimum 3 resources must have ODM Level Certification (preferably any or combination of the proposed OEM).	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
294	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. Greater than 7 Years -> 10 Marks Greater than 5 Years up to 7 Years -> 7 Marks Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company/OEM should have relevant implementation and operational experience for similar SOC tools to PSU/Government/Private/BFSI Sector Firms in India. Greater than 7 Years -> 10 Marks Greater than 5 Years up to 7 Years -> 7 Marks Greater than 3 Years up to 5 Years -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
295	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 2 references of 65000 IP Addresses and above -> 10 Marks 2 references of 50000 IP Addresses and above -> 7 Marks 2 references of 25000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Request to modify the clause as: The bidder or bidder's parent company or OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for minimum of: 2 references of 25000 IP Addresses and above -> 10 Marks 2 references of 10000 IP Addresses and above -> 7 Marks 2 references of 5000 IP Addresses and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
296	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 3 references and above -> 10 Marks 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms in India for minimum of: 3 references and above -> 10 Marks 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
297	Annexure D: Technical Scoring	Annexure D: Technical Scoring	115	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 3 references and above -> 10 Marks 2 references and above -> 5 Marks	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution or extreme SSL acceleration upgrades to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 3 references and above -> 10 Marks 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
298	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 2 references of 10000 users and above -> 10 Marks 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM during the last 7 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: 2 references of 5000 users and above -> 10 Marks 2 references of 5000 users and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
299	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India 4 references -> 10 Marks 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms in India 4 references -> 10 Marks 2 references -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
300	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India 4 references -> 5 Marks 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India 4 references -> 5 Marks 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
301	Annexure D: Technical Scoring	Annexure D: Technical Scoring	116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India 4 references -> 5 Marks 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Kindly modify the clause as: The bidder or bidder's parent company /OEM must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India 4 references -> 5 Marks 2 references -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	Please refer to the revised "Annexure D"
302	1. Brief Scope of Work	Planning	50	Ensure compatibility and interoperability between different security solutions.	Kindly provide the details of existing security solution to verify the compatibility and interoperability.	The details shall be shared with the successful bidder
303	1. Brief Scope of Work	Training & Certification	54	Bidder shall train specified LIC employees for operational Management of the system. Training shall be provided on each of the following modules to specified LIC personnel. Training shall be provided at no additional cost to LIC through OEM approved authorized agencies/facilities. All trainings have to be imparted at LIC's premises.	Kindly provide the number of batches and size of batch for training.	Please refer to the revised "Section E: Scope of Services"
304	1. Brief Scope of Work	Mobile Device Management (MDM)	59	Create, update, and delete access control rules, groups, and policies in WAF after obtaining approval.	We understand that this is related to WAF section not the MDM. Please confirm	Please refer to the revised "Section E: Scope of Services"

305	1. Brief Scope of Work	API Gateway, Management and Security	62	On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management.	Kindly clarify if we need to manage existing API security gateway solution.	API Gateway and Security Solution has been removed from the scope of this RFP
306	2. Detailed Scope of Work	I. General Requirements	62	All the solutions should be seamlessly integrated with the LIC's NTP solution and must be compatible with any provided NTP version.	Request to provide existing NTP details for integration validation.	The details shall be shared with the successful bidder
307	2. Detailed Scope of Work	VIII. Mobile Device Management (MDM)	69	The vendor should deploy API Gateway, Management and Security solution within the organization's network.	We understand that this is related to API Gateway section not the MDM. Please confirm	Please refer to the revised "Section E: Scope of Services"
308	5. Resource Deployment	Project Coordinator	73		Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
309	5. Resource Deployment	Network Access Control (NAC)	73	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
310	5. Resource Deployment	Network Access Control (NAC)	73	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
311	5. Resource Deployment	SSL Offloader	74	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
312	5. Resource Deployment	SSL Offloader	75	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
313	5. Resource Deployment	Web Application Firewall (WAF)	76	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
314	5. Resource Deployment	Web Application Firewall (WAF)	76	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	We understand 2 resources required at each shift. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
315	5. Resource Deployment	Mobile Device Management (MDM)	77	L2 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
316	5. Resource Deployment	Mobile Device Management (MDM)	77	L1 Security Analyst – 2 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
317	5. Resource Deployment	API Gateway, Management and Security	78	L2 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	API Gateway and Security Solution has been removed from the scope of this RFP
318	5. Resource Deployment	API Gateway, Management and Security	79	L1 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	API Gateway and Security Solution has been removed from the scope of this RFP
319	5. Resource Deployment	Virtual Desktop Interface (VDI)	80	L3 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
320	5. Resource Deployment	Virtual Desktop Interface (VDI)	80	L1 Security Analyst – 1 (24x7 shift) at LIC Central Office, Mumbai	Please define the shift/ working time	Please refer to the revised "Section E: Scope of Services"
321	5. Resource Deployment	Remote (offsite) Support	86	The successful Bidder has to provide throughout the contract period, the services of an offsite support beyond LIC's office hours. The roles and responsibilities of offsite support would be the same as that of onsite support as mentioned above.	Kindly clarify Remote support person need to be dedicated or shared resource	Please refer to the revised "Section E: Scope of Services"
322	5. Resource Deployment	Remote (offsite) Support	86	The offsite support has to monitor using the VPN setup at vendor end at vendors cost.	We understand that LIC will provide VPN access via SSL client for remote monitoring. Kindly confirm	Please refer to the revised "Section E: Scope of Services"
323	Annexure F - Technical Compliance VDI Pointers		40	NA	The solution should be able to encrypt end to end traffic from end user to network to controller/broker Since Broker remains in LAN and connect VDI server in LAN only, the encryption requirement should be from end-point to Gateway (Hosted in DMZ). Hence requesting you to consider following modifications: Modified lines should be: The solution should be able to encrypt end to end traffic from end user to network to "Gateway"	Please refer to the revised "Annexure F"
324	Annexure F - Technical Compliance VDI Pointers		49	NA	The solution must support block saving and uploading of any file to any server location including user's personal desktop and my documents folders Expectation in line is not clear, request to add sepeck requirement as below for clarification. Modified lines should be: The solution must support block saving and uploading of any file "from end point" to any server location including user's personal desktop and my documents folders In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent advancement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool Audio & Video. Also Flash is no more in use please remove it.	Please refer to the revised "Annexure F"
325	Annexure F - Technical Compliance VDI Pointers		66	NA	The solution should have the ability to offload rendering of video and flash content to endpoint when the endpoint is capable In VDI all computing happened on server using server resource Video will also use server media player for to open video files, however recent advancement has decoupled collaboration tool's audio & video offloading to end-point, please modify and put collaboration tool Audio & Video. Also Flash is no more in use please remove it. Modified lines should be: The solution should have the ability to offload rendering of "Teams, Zoom, Webex Voice / video" and flash content to endpoint when the endpoint is capable	Please refer to the revised "Annexure F"
326	Annexure F - Technical Compliance VDI Pointers		73	NA	The solution should support HTML5 based clientless access with printing and peripheral USB devices redirection to support e-Tokens, native printing HTML5 based clientless can provide VDI access but browser does not have capability to redirect USB, Printer etc, hence Plugin is essential. Request to add plugin to this point. Modified lines should be: The solution should support HTML5 based clientless access and "plugin based" printing and peripheral USB devices redirection to support e-Tokens, native printing	Please refer to the revised "Annexure F"
327	Annexure F - Technical Compliance VDI Pointers		76	NA	The solution should be able to provide a launch and access to a virtual application in less than 5 seconds on LAN environment. Launch time of VDI depends on many factors, like AD, Group policy, printer and drive mapping it requires more times than default desktop, 5 second login time is unachievable, please modify it to minimum 25 sec. Modified lines should be: The solution should be able to provide a launch and access to a virtual application in less than 5 between (25 to 50 second) seconds on LAN environment.	Please refer to the revised "Annexure F"
328	Annexure C - Eligibility criteria		Page 113/Sr.No. 8	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	The clause implies that the bidders should have implemented proposed OEM VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India Modified Clause should be "bidders should have implemented any VDI for a minimum of 50 users to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
329	Section G - Payment Terms & Conditions		Page 104	Point No 3 - Payment schedule table	As we will be supplying perpetual license at the beginning, 100% license cost should be paid once licenses are delivered and invoices raised.	Please refer to the revised "Payment Terms & Conditions"
330	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	3	Device should be based on dedicated <2U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40 vCPUs scalable to 60 vCPU's.	Query: I. RFP has asked for Less than 2RU i.e. 1RU form factor for Proposed appliance, which is not true for all OEM, i.e. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size of CPU which changes the need of number of vCPUs and cannot be binding factor and due to this request to relax the specs Hence we request to relax the requirement to below Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
331	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	4	Should have minimum SSL visibility throughput of 146 Gbps from day 1 and scalable to 195 Gbps on same platform with hardware compression.	Suggestion: for the SSL offloader technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill Hence request to change the specs to below: Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities	Please refer to the revised "Annexure F"
332	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	5	Should support minimum SSL Visibility TPS: -300 K TPS (RSA 2k keys) from day 1 and scalable to 400 K TPS (RSA 2k Keys) on same platform -180 K TPS (ECDHE-ECDSPA-256) from day 1 and scalable to 300 K TPS (ECDHE-ECDSPA-256) on same platform	Suggestion: The asked SSL CPS/TPS in the specs seems to be overkill compared to current and future growth and specific to single OEM Hence request to change the specs to below: Should support minimum SSL Visibility TPS: -120 K TPS (RSA 2k keys) from day 1 on same platform -70 K TPS (ECDHE-ECDSPA-256) from day 1 on same platform	Please refer to the revised "Annexure F"
333	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR		The SSL Off loader must have the minimum 40 vCPUs from day 1 and scalable to 60 vCPUs on same platform Memory: 512 GB DDR4 Storage: 1 TB SSD	Suggestion: Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and due to this request to relax the specs Hence request to relax the specs to below The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please refer to the revised "Annexure F"
334	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	7	The proposed solution should have a 45 Gbps bulk encryption from Day 1 and scalable to 100 Gbps bulk encryption	Suggestion: Having such high SSL throughput for 100Gbps seems to be overkill Hence request to change the specs to below: The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F"
335	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appliance due to unpredictable traffic flow and increases troubleshooting complexity Hence request to change the specs to below The SSL offloader solution must support 1+1 inline tool redundancy for inline tools	Please refer to the revised "Annexure F"

336	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	18	The Solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM Hence request to change the specs to below The Solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"
337	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicitly proxy) functionality with add-on licenses if required in future	Query: The features asked in the specs seems to be specific to particular OEM and below technology seems not to be related to SSO Solution - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicitly proxy) functionality Hence request to change the specs to below SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
338	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-In-The-Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
339	Annexure F - Technical Compliance	SSL Offloader Tech Specs DC-DR	81	The SSL Offloader device should be able to have flexible ICAP request or respond policies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	This is specific to a single OEM, hence request to change the specs to below The SSL Offloader device should be able to have flexible ICAP request or respond policies.	Please refer to the revised "Annexure F"
340	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	3	Device should be based on dedicated 1U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 4 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24 vCPUs scalable to 36 vCPUs	Query: 1. RFP has asked for Less than 2RU i.e. 1RU form factor for Proposed appliance, which is not true for all OEM, 2. Amount of vCPU asked on same appliance depends on OEM, as every OEM have different way of working, and different size of CPU which changes the need of number of vCPUs and cannot be binding factor and due to this request to relax the specs Hence we request to relax the requirement to below Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum of 2 x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 16 CPU	Please refer to the revised "Annexure F"
341	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	4	Should have minimum SSL visibility throughput of 115 Gbps from day 1 and scalable to 175 Gbps on same platform with hardware compression.	Suggestion: for the SSO like technology having such high throughput of 146Gbps Scalable to 195G seems to be overkill Hence request to change the specs to below: Should have minimum SSL visibility throughput of 120 Gbps from day 1 on same platform with compression capabilities Suggestion: Amount of vCPU, Memory and Storage Needed on same appliance depends on OEM, as every OEM have different way of working and cannot be binding factor and due to this request to relax the specs	Please refer to the revised "Annexure F"
342	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR		The SSL Off loader must have the minimum 24 vCPUs from day 1 and scalable to 36 vCPU's on same platform Memory: 256GB DDR4 Storage: 1 TB SSD	Hence request to relax the specs to below The SSL Off loader must have the minimum 16 CPU on same platform Memory: 192 GB DDR4 Storage: 500G SSD	Please refer to the revised "Annexure F"
343	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	7	The proposed solution should have a 65 Gbps bulk encryption from Day 1 and scalable to 85 Gbps bulk encryption	Suggestion: Having such high SSL throughput for 100Gbps seems to be overkill Hence request to change the specs to below: The proposed solution should have a 45 Gbps bulk encryption from Day 1	Please refer to the revised "Annexure F"
344	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	14	The SSL offloader solution must support N+1 and 1+1 inline tool redundancy for inline tools.	Feature asked seems to be clustering which is not desired feature for Network appliance due to unpredictable traffic flow and increases troubleshooting complexity Hence request to change the specs to below The SSL offloader solution must support 1+1 inline tool redundancy for inline tools.	Please refer to the revised "Annexure F"
345	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	18	The Solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same 1RU rack appliance	Having 1RU form factor seems to be specific to single OEM Hence request to change the specs to below The Solution must support both inbound SSL/TLS Protocol decryption and outbound SSL/TLS Protocol decryption capabilities concurrently within the same appliance	Please refer to the revised "Annexure F"
346	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	39	SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSO device should be able to also perform URL Filtering, IP intelligence, HSM integration, Zero trust application access with SAML/Oauth with MFA and Secure web gateway (explicitly proxy) functionality with add-on licenses if required in future	Query: The features asked in the specs seems to be specific to particular OEM and below technology seems not to be related to SSO Solution - Zero trust application access with SAML/Oauth with MFA - Secure web gateway (explicitly proxy) functionality Hence request to change the specs to below SSL Orchestrator should provide an all-in-one appliance solution designed specifically to optimize the SSL infrastructure, provide security devices with visibility of SSL/TLS encrypted traffic, and maximize efficient use of that existing security investment. This solution should support policy-based management and steering of traffic flows to existing security devices, designed to easily integrate into existing architectures, and centralizes the SSL decrypt/encrypt function by delivering the latest SSL encryption technologies across the entire security infrastructure. The SSO device should be able to also perform URL Filtering, IP intelligence, HSM integration	Please refer to the revised "Annexure F"
347	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	43	The Proposed solution must provide capabilities to obfuscate sensitive field names in an application to defeat Man-In-The-Browser Attacks on the device itself if required in future via add on licenses	This is specific to a single OEM, hence request to delete the specs	Please refer to the revised "Annexure F"
348	Annexure F - Technical Compliance	SSL Offloader Tech Specs NDR	81	The SSL Offloader device should be able to have flexible ICAP request or respond policies. 1. Enabling ICAP only for HTTP response traffic (It may be useful in some scenarios to only send HTTP response traffic to ICAP, as the vast majority of HTTP GET requests are devoid of payloads.) 2. Enabling ICAP only for HTTP POST request traffic (POST requests will generally always contain a payload, while GET requests usually will not.) 3. Enabling ICAP only for HTTP POST request and all response traffic (This rule will enable ICAP processing on POST requests, all HTTP responses, and would typically be used to filter out normally empty GET and other types of requests.) 4. Enabling ICAP for specific request URL extensions and response content types (Sometimes you just need to activate ICAP for specific file type requests - request URLs that end with something like ".exe", ".sh", or ".bat", and also only scan responses of a specific MIME types (HTTP Content-Type) like "application/json" and application/executable)	This is specific to a single OEM, hence request to change the specs to below The SSL Offloader device should be able to have flexible ICAP request or respond policies.	Please refer to the revised "Annexure F"
349	SSL Offloader Tech Specs DC-DR			The solution should support minimum SSL Visibility TPS - 260 K TPS (RSA 2k keys) Scalable to 400 K TPS (RSA 2k keys) - 180 K TPS (ECDHE-ECDSA P-256) Scalable to 300 K TPS (ECDHE-ECDSA P-256) on the same hardware	The RFP has requested 30,000 SSL TPS for the Web Application Firewall, which seems reasonable. The largest payment transactions interface in India has SSL TPS of no more than 50,000. Also, major organizations, like big banks, don't have SSL TPS exceeding 50,000. The SSL TPS requested for SSO seems excessively high and unrealistic, leading to an oversized requirement. We kindly request you to amend this point "The solution should support minimum SSL Visibility TPS - 100 K TPS (RSA 2k keys) Scalable to 150 K TPS (RSA 2k keys) Scalable to 100 K TPS (ECDHE-ECDSA P-256) Scalable to 100 K TPS (ECDHE-ECDSA P-256) on the same hardware with license upgrade"	Please refer to the revised "Annexure F"
350	SSL Offloader Tech Specs DC-DR			Device should be based on dedicated <2U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 40vCPU scalable to 60 vCPUs	vCPU stands for "Virtual Central Processing Unit", denoting a virtualized CPU assigned to a virtual machine (VM) within a virtualized environment. These logical processing units are vital for supplying computational resources to virtualized environments. Notably, virtualization is not a prerequisite for SSL Offloading (SSLO). However, it's worth noting that currently, only one OEM offers a CPU hardware appliance. Additionally, the interface and CPU requirements specified in the RFP are tailored to one OEM, potentially impeding the participation of well-known "Make in India" OEMs. Therefore, we kindly request modifying this point to: "Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC Platform. The Platform should have a minimum 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 2x32Core processor"	Please refer to the revised "Annexure F"
351	SSL Offloader Tech Specs NDR			Device should be based on dedicated 1U hardware appliance, this should be dedicated offering from the client and not part of ADC platform. The platform should have a minimum 4x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 24vCPU scalable to 36 vCPUs	vCPU stands for "Virtual Central Processing Unit", denoting a virtualized CPU assigned to a virtual machine (VM) within a virtualized environment. These logical processing units are vital for supplying computational resources to virtualized environments. Notably, virtualization is not a prerequisite for SSL Offloading (SSLO). However, it's worth noting that currently, only one OEM offers a 1U hardware appliance with this specifications. Additionally, the interface and CPU requirements specified in the RFP are tailored to one OEM, potentially restrict the participation of well-known "Make in India" OEMs. Therefore, we kindly request modifying this point to: "Device should be based on dedicated hardware appliance, this should be dedicated offering from the client and not part of ADC Platform. The Platform should have a minimum 2x100G/40G QSFP28/QSFP+, 16x25G/10G SFP28/SFP+ ports from day1, Processor: Minimum 2x32Core processor"	Please refer to the revised "Annexure F"
352	Section C	Annexure R	19		Quantity of WAF gateways and Management systems are not mentioned in Annexure R Bill of Quantity	Please refer to the revised "Section E: Scope of Services"
353	Section H	Annexure F, 1D		For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS, TACACS+ or via local table of authorized users	Request to modify the clause as "For access via CLI (console, telnet, SSH) WBM and Web Services (HTTPS) users can be authenticated via RADIUS/TACACS+ via local table of authorized users"	Please refer to the revised "Annexure F"
354	Section H	Annexure F, 86		The solution must protect system against WASC Web Security Attack classification.	Request to modify the clause as "The solution must protect system against WASC Web Security Attack classification or OWASP top 10"	Please refer to the revised "Annexure F"
355	Additional Points			Proof of Concept (POC) in Live environment The LIC at its discretion may ask for the Proof-of-Concept/Value (POC/POV) of the proposed solution in the production set up with the bidders whose bids are technically qualified. 1. The LIC will provide a couple of week's time for conducting POC/POV at LIC's production environment for the solution proposed in the tender. 2. The LIC may raise certain clarifications during evaluation and the respective bidder should provide the response as per timelines stipulated from time to time without which the bid will be treated as incomplete and may be rejected. 3. Failing to comply with the requirements of the LIC as mentioned in the Tender document or if the solution does not fit into the LIC's production setup due to any third party dependencies etc. then the bid will be treated as incomplete and may be rejected.	Live Proof of Concept (POC) is important for Network Access Control (NAC) projects for several reasons: 1. Validation of Functionality: It allows LIC to validate that the proposed NAC solution works as intended in their specific environment. This ensures that the solution meets the LIC's requirements and effectively addresses the security needs. 2. Identification of Challenges: Live POC helps identify any potential challenges or issues that may arise during deployment or operation. This allows for troubleshooting and fine-tuning before full implementation, minimizing disruptions and optimizing performance. 3. Risk Mitigation: Live POC allows organizations to assess the risks associated with implementing a new NAC solution in LIC environment before committing to a full rollout. This proactive approach helps mitigate potential security vulnerabilities and operational risks. Conducting a live POC for a NAC project helps ensure successful deployment, minimize risks, and optimize the solution to meet the organization's specific requirements.	Please refer to the revised "Technical Bid Evaluation"

356	Annexure F - API Technical Specification				Is there a need for API Manager to provide a multi-tenant solution for different set and owners of APIs using a single deployment and having a centralised portal for managing the same.	API Gateway and Security Solution has been removed from the scope of this RFP
357	Section E - Scope of Services - Ongoing Requirements	Pg 70	API Gateway Management and Security - 1000 APIs		What is the overall transaction per second TPS requirement that will need to be supported by the Gateway Component	API Gateway and Security Solution has been removed from the scope of this RFP
358	Annexure F - API Technical Specification	Pt 1	The solution should be an end-to-end API Gateway, Management and Security solution.		Is API Mgmt. Solution, for the API security, expected to be preintegrated & bundled along with Security Solution like SSO, OAuth2, SAML, etc.	API Gateway and Security Solution has been removed from the scope of this RFP
359	Annexure F - API Technical Specification				Does the solution requires flexibility to deploy multiple API gateways as required & managed using Single Central API Manager at no additional cost of the APGateway component. This could include internal and External APIs	API Gateway and Security Solution has been removed from the scope of this RFP
360	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway, Management and Security -	Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.		Does the integration platform need to be light weight, modular, with subatomic startup time, with low footprint reusable extensions and cloud native based on latest technologies like Quarkus with OOTB Connectors and Extension to connect to existing and modern technologies.	API Gateway and Security Solution has been removed from the scope of this RFP
361	Annexure F - API Technical Specification				Kindly confirm if the proposed solution should support microservices architecture and capable of running as container images, cloud ready.	API Gateway and Security Solution has been removed from the scope of this RFP
362	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway, Management and Security -	Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.		Does the solution expects the components to be cloud native containerised deployment across Hybrid Cloud on container platform?	API Gateway and Security Solution has been removed from the scope of this RFP
363	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway, Management and Security -	Pg 68	The vendor should provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.		Does the solution expects the application/components deployed across Hybrid cloud (Onpremises & Public/Private Cloud) to be managed & secured with single pane of glass	API Gateway and Security Solution has been removed from the scope of this RFP
364	Section E - Scope of Services - 2. Detailed Scope of Work - VII - API Gateway, Management and Security -	Pg 68	24x7 real-time monitoring uptime, availability, health performance of API Gateway, Management and Security devices with mitigation support.		As part of Enterprise Logging & Observability, is it expected functionality to have preintegrated logging & observability functionality as part of underlying platform	API Gateway and Security Solution has been removed from the scope of this RFP
365	Annexure F - API Technical Specification	Pt 2B	The Solution should be built to support CI/CD.		Does the solution expect DevSecOps tools to be preintegrated & bundled as part of underlying platform and should not have any additional license/subscription cost to LIC?	API Gateway and Security Solution has been removed from the scope of this RFP
366	Section E - Scope of Services - 1. Brief Scope of Work - On-Site Support Services VII - API Gateway, Management and Security -	Pg 62	The change management of all the devices must be adhering to standards and policies of LIC.		Is there any need for automation tool for installation, patching, configuration mgmt of the components and platforms using a centralised system for all environments including DC, DR, UAT	API Gateway and Security Solution has been removed from the scope of this RFP
367	3. Technical Bid	Pg 22	The bidder must supply a thorough inventory of the hardware components required for the planned implementation of the in-scope solutions. This bill of Quantity (BoQ) as per Annexure R should be itemized separately for all the environments, including DC, UAT and Disaster Recovery (DR).		Are DC, DR and UAT only environments or are there any other environments as well, like Dev, SIT, Pre-Prod, etc.	Please refer to the revised "Section E: Scope of Services" and Revised "Technical Bid"
368	Annexure F - Technical Compliance	CASB Technical Specifications	The proposed CASB Solution must have at least 5 x Full Compute Edge DC's / POPs / Locations in India to cater DC, DR and NDR scenarios.		The CASB architecture has an edge/POP architecture where our users get connected to the nearest edge location wherever the cloud exists to get connected to our PoP, would request LIC to consider this architecture We have currently 2 POP locations and 4 edge locations	Please refer to the revised "Annexure F"
369			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats.		CASB provides restricted access to application based on configured rules and hence does not need an IPS functionality	Please refer to the revised "Annexure F"
370			The solution must have Web IPS (Signatures) to protect against targeted user-agent threats.		CASB provides restricted access to application based on configured rules and hence does not need an IPS functionality	Please refer to the revised "Annexure F"
371	Accesure C - Eligibility Criterion	112/113	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.		Request to change to -The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 3 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
372	Accesure C - Eligibility Criterion	112/113	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.		request to change to -The Bidder during the last 5 years preceding to the date of this RFP should have implemented, and supported the Network Access Control (NAC) OEM to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
373	Accesure C - Eligibility Criterion	112/113	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.		Request to change to -The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
374	Accesure C - Eligibility Criterion	112/113	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India		Request to change to -The bidder during the last 5 years preceding to the date of this RFP should have supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
375	Accesure C - Eligibility Criterion	112/113	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India for minimum of:		Request to change to -The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM / OR API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
376	Accesure C - Eligibility Criterion	112/113	The Bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.		EIT will request for this eligibility clause to be removed	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
377	Accesure D - Technical scoring	115/116	Annual turnover during the last 03 (three) years preceding the date of this RFP. ⊕ Greater than INR 500 Crore -> 10 Marks ⊕ Greater than INR 300 Crore up to INR 500 Crores -> 7 Marks ⊕ Greater than INR 100 Crore up to INR 300 Crores -> 5 Marks		Request to change to - Annual turnover during the last 03 (three) years preceding the date of this RFP. ⊕ Greater than INR 1000 Crore -> 10 Marks ⊕ Greater than INR 500 Crore up to INR 1000 Crores -> 7 Marks ⊕ Greater than INR 300 Crore up to INR 500 Crores -> 5 Marks	Please refer to the revised "Annexure D"
378	Accesure D - Technical scoring	115/116	The Bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. ⊕ Greater than 7 Years -> 10 Marks ⊕ Greater than 5 Years up to 7 Years -> 7 Marks ⊕ Greater than 3 Years up to 5 Years -> 5 Marks		Request to change to -The bidder should have relevant implementation and operational experience for in scope tools to PSU/Government/Private/BFSI Sector Firms ⊕ Greater than 7 Years -> 10 Marks ⊕ Greater than 5 Years up to 7 Years -> 7 Marks ⊕ Greater than 3 Years up to 5 Years -> 5 Marks	Please refer to the revised "Annexure D"
379	Accesure D - Technical scoring	115/116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⊕ 2 references of 65000 IP Addresses and above -> 10 Marks ⊕ 2 references of 50000 IP Addresses and above -> 7 Marks ⊕ 2 references of 25000 IP Addresses and above -> 5 Marks		Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied OR implemented OR supported NAC solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⊕ 2 references > 10 Marks ⊕ 1 references > 7 Marks	Please refer to the revised "Annexure D"
380	Accesure D - Technical scoring	115/116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⊕ 3 references and above -> 10 Marks ⊕ 2 references and above -> 5 Marks		Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied OR implemented OR supported WAF solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⊕ 3 references and above -> 10 Marks ⊕ 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
381	Accesure D - Technical scoring	115/116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⊕ 3 references and above -> 10 Marks ⊕ 2 references and above -> 5 Marks		Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, OR implemented OR supported SSL Offloader solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⊕ 3 references and above -> 10 Marks ⊕ 2 references and above -> 5 Marks	Please refer to the revised "Annexure D"
382	Accesure D - Technical scoring	115/116	The Bidder during the last 5 years preceding to the date of this RFP, must have supplied, implemented and supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India for minimum of: ⊕ 2 references of 10000 users and above -> 10 Marks ⊕ 2 references of 5000 users and above -> 5 Marks		Request to change to -The Bidder during the last 5 years preceding to the date of this RFP, must have supplied OR implemented OR supported MDM solution to clients in the PSU/Government/Private/BFSI Sector Firms : ⊕ 1 references of 10000 users and above -> 10 Marks ⊕ 1 references of 5000 users and above -> 5 Marks	Please refer to the revised "Annexure D"
383	Accesure D - Technical scoring	115/116	The bidder must have supplied, installed, implemented, and managed the API Gateway, Management and Security solution for a minimum of 500 APIs in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⊕ 4 references -> 10 Marks ⊕ 2 references -> 5 Marks		EIT will request that the scoring criteria to be removed	Please refer to the revised "Annexure D"
384	Accesure D - Technical scoring	115/116	The bidder must have supplied, installed, implemented, and managed the CASB solutions for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⊕ 4 references -> 5 Marks ⊕ 2 references -> 2 Marks		EIT will request that the scoring criteria to be removed	Please refer to the revised "Annexure D"
385	Accesure D - Technical scoring	115/116	The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India ⊕ 4 references -> 5 Marks ⊕ 2 references -> 2 Marks		The bidder must have supplied, installed, implemented, and managed the VDI solution for a minimum of 100 users in the PSU/Government/Private/BFSI Sector Firms in India ⊕ A Reference having more than 1000 users -> 5 Marks ⊕ A Reference having more than 500 users and less than 1000 users -> 2 marks	Please refer to the revised "Annexure D"

386	6. Eligibility Criteria	Point No.04	14	The Bidder should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The Bidder/OEM should have minimum of 3 years of experience in supplying, implementing, and supporting minimum 4 out of the 7 in-scope solutions related to this RFP to organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
387	6. Eligibility Criteria	Point No.05	14/15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented, and supported the Network Access Control (NAC) OEM for a minimum of 25,000 IP Addresses to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India. The proposed OEM product for NAC should have been successfully running in minimum 02 (two) organizations with minimum 500 branches distributed across India of minimum 25,000 IP Addresses in the last 05 (five) years preceding to the date of the RFP.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
388	6. Eligibility Criteria	Point No.06	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Web Application Firewall (WAF) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
389	6. Eligibility Criteria	Point No.07	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Mobile Device Management (MDM) / SSL Offloader (SSLO) to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
390	6. Eligibility Criteria	Point No.08	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Virtual Desktop Interface (VDI) OEM for a minimum of 50 users / API Gateway, Management and Security for a minimum of 100 APIs to at least 02 (two) organisations in PSU / Government / Private / BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
391	6. Eligibility Criteria	Point No.09	15	The bidder during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	We kindly request you to modify the clause as follows: The bidder/OEM during the last 5 years preceding to the date of this RFP should have supplied, implemented and supported the Cloud Access Service Broker (CASB) to at least 02 (two) organisations in PSU/Government/Private/BFSI Sector Firms with more than 500 branches across different locations in India.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"
392	6. Eligibility Criteria	Point No.10	15	The bidder must have a minimum of 15 IT Security permanent professionals with experience in-scope solutions on their payroll with certifications such as CISSP / OSCP / CEH / CCNP / CISA / CISM / OEM Level Certification. Minimum 3 resources must have OEM Level Certification (preferably of the proposed OEM).	We kindly request you to modify the clause as follows: The bidder must have a minimum of 25 IT Security permanent professionals on their payroll with certifications.	Please refer to the revised "Annexure C and Minimum Eligibility Criteria"