Section E: Scope of Services

1. Brief Scope of Work

A. As part of this RFP, LIC intends to implement the following solutions / services at LIC:
   I. Cloud Access Security Broker (CASB)
   II. Network Access Control (NAC)
   III. SSL Off loader (SSLO)
   IV. Web Application Firewall (WAF)
   V. Virtual Desktop Infrastructure (VDI)
   VI. Mobile Device Management (MDM)
   VII. Server Load Balancer (SLB)

B. The bidder shall perform the below high-level activities as part of the scope of work. Please note, the below list of activities is only indicative and not an exhaustive list. The deliverables mentioned shall be provided for each solution as part of this RFP.

Phase No.	Phase Name	Activities to be performed	Deliverables
1	**Planning**	• Conduct kick-off meeting. • Study of present architecture at Data centers. • Study of LIC's existing security environment and guidelines. • Identify business objectives & technical requirements. • Define pre-requisites if any. • Outline an implementation strategy and detailed plan with timelines and milestones for entire duration of the project. • Ensure that security and compliance requirements are integrated into the design and develop a plan for addressing them. • Ensure compatibility and interoperability between different security solutions. • Define the allocation of resources including personnel, equipment, and tools. • Outline the accurate placement of devices or appliances to ensure industry best practices are followed. • Conduct workshops with all the departments of LIC and any other identified vendor for (but not limited to) solution engineering, identifying gaps, crown jewels of LIC, integration, custom parser creation, creation of rules, use case development, finetuning, etc.	Detailed Project Plan for each solution as part of this RFP. Note: Separate plan document to be submitted for each in-scope solution.

Phase No.	Phase Name	Activities to be performed	Deliverables
2	**Designing**	• **Architecture Diagram:** o Design the overall implementation architecture (high-level diagram and low-level diagram) for each in-scope solution. o Connectivity and data flow diagram for each in-scope solution. • **Policy & Procedure Documents:** o SOP for solution implementation. o SOP for operations of the solution. o Detailed roles and responsibilities defined in RACI matrix. o Minimum Baselines Standard Document (MBSS)/Secure Configuration Document (SCD). o Access controls and security measures implemented document. o Acceptance procedures, Test cases & test plans, etc. o BCP/DR/Failover Strategy and process document. o Incident Response strategy and process document.	• Architecture Diagrams (High-level and low-level) • Connectivity and data flow diagram • Policy & Procedure documents Note: Above documents shall be prepared in a mutually agreed template. Bidder shall submit soft and hard copies for all the above documents in the finalized template.
3	**Implementing**	• **Supply and Installation:** o Supply of appliances wherever applicable and software for in-scope solutions. o Installation and implementation of the solutions as per the architecture design. o Installation will include proper mounting, labeling, tagging of all the equipment. o The bidder is responsible for determining the appropriate hardware sizing. LIC will supply the server, rack space, and cooling. The bidder is also responsible for furnishing any other necessary hardware or equipment to ensure smooth integration of all the in-scope solutions. As per LIC's requirement, the successful bidder of the project shall be ready to shift, occasionally, the equipment from one place to other, uninstall and reinstall all the equipment without any additional cost to LIC. • **Configuration & Integration:**	• Site Ready Document/Site Not Ready Document as applicable. • Successful deployment confirmation • Validation report by OEM

Phase No.	Phase Name	Activities to be performed	Deliverables
		o Configuring the solutions as per defined MBSS/SCD. Configuration to meet industry standards and regulatory guidelines. o Integrating the solutions with: • Its own components as applicable. • Other security solutions as applicable. • Active directory, servers, network devices, endpoints, and other applicable IT assets. o Bidder shall recommend ways for secure communication and assist LIC in defining the firewall rules as applicable. All such configurations shall be documented as part of the policy/process documentation. Configuration of firewall rules will be done by LIC firewall team. o Bidder shall provide the details of all scripts and configurations created or used at LIC, including their purpose, functionality, and relevance to the scope of work. • **Optimizing & Deployment Validation:** o Fine 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. o Monitor and resolve issues as per the defined SLAs in this RFP. o Validation of deployment of the solutions/services to be performed based on industry best practices by respective OEM of the deployed solution/service. In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a separate report to LIC accordingly. Bidder shall perform necessary changes as recommended by the OEM. o The OEM is required to conduct the audit, at the end of implementation and once in end of every year during	

Phase No.	Phase Name	Activities to be performed	Deliverables
		the contract period. The recommendations/ remediation changes required after each audit should be completed within 3 months. o Bidder should discuss about the Governance structure and Project milestones and provide weekly updates to LIC on implementation status.	
4	**Sustaining**	• Post- deployment (after sign-off from LIC) bidder shall manage & monitor proposed solutions. • Facilitation & operation for continuous monitoring, performance optimization, upgradation, maintaining compliance with LIC policies, industry standards and regulatory guidelines, change management, incident response, etc.	• Periodic reports such as (but not limited to) Daily, Monthly, Weekly, Adhoc, Audit requirement reports, etc. • Dashboards

C. Compliance with IS Security Policy:

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. Some of the key areas are as under:

- o Responsibilities for data and application privacy and confidentiality.
- o Responsibilities on system and software access control and administration
- o Custodial responsibilities for data, software, hardware, and other assets of LIC being managed by or assigned to the Vendor
- o Physical Security of the facilities
- o Physical and logical separation from other customers of the Vendor
- o Incident response and reporting procedures
- o Password Policy
- o Access management Policy
- o Acceptable usage Policy (Authentication and Identity Management, Authorization, and access control)
- o Data Encryption / Protection requirements of LIC
- o Cyber Security Policy
- o Auditing
- o In general, confidentiality, integrity and availability, non-repudiation, authenticity, privacy of data/information must be ensured
- o Responsibilities in carrying out background verification of personnel deployed from vendor side regularly and submit the report as and when needed by LIC

D. Right to Audit:

i. It is agreed by and between the parties that the Service Provider shall get itself annually audited by external empaneled Auditors appointed by LIC/ inspecting official from the IRDAI or any regulatory authority, covering the risk parameters finalized by LIC/ such auditors in the areas of products (IT hardware/ software) and services etc. provided to LIC and the vendor shall submit such certification by such Auditors to LIC. The vendor and or

his / their outsourced agents /sub – contractors (if allowed by LIC) shall facilitate the same. LIC can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by LIC.

ii. Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by LIC or in the certification submitted by the Auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. It is also agreed that the Service Provider shall provide certification of the auditor to LIC regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies observed. All costs for such audit shall be borne by the service provider/vendor.

iii. Service Provider further agrees that whenever required by LIC, it will furnish all relevant information, records/data to such auditors and/or inspecting officials of the LIC/ IRDAI and or any regulatory authority required for conducting the audit. LIC reserves the right to call and/or retain for any relevant material information / reports including audit or review reports undertaken by the Service Provider (e.g., financial, internal control and security reviews) & findings made on the Service Provider in conjunction with the services provided to LIC.

E. Documentation

i. All the documents shall be supplied in properly bound volumes of A4 size sheets.

ii. Three sets of hardcopies as applicable and one softcopy on CD shall be supplied as final document.

iii. Documents for high level design, detailed design, configuration of individual features set on various appliances, general testing, scenario-based fail-over testing, Standard Operating Procedure, best practices etc. shall form the complete set for fulfilling the documentation criteria.

iv. Vendor shall also submit Delivery and Installation Report, Warranty certificates, License Copies for all the items supplied along with the supplies.

v. Installation report should contain the part numbers of all the components supplied by the selected bidders.

F. Training & Certification

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/faculties. All trainings have to be imparted at LIC's premises for maximum 25 participants.

i. Pre-Implementation: Provide training to the LIC personnel/ Onsite support team on the product architecture, functionality, and the design for each solution under the scope of this RFP.

ii. Post Implementation: Provide hands-on training to the LIC personnel/ Onsite support team on day-to-day operations, alert monitoring, policy configuration, rule creation, report generation for all solutions etc.

iii. Documentation and knowledge transfer after each patch/version update.

iv. The bidder and OEM/OEM approved Authorized agencies/faculties are required to provide training jointly table for people nominated by the LIC for each solution specified in the scope of work.

v. The bidder and OEM/OEM certified partners are required to provide ad-hoc trainings to the LIC staff as required by LIC, to acquaint them with the latest features and functionalities of the solutions for minimum of one day. LIC has the right to exercise this training option at its discretion.
vi. The bidder is required to provide all trainees with detailed training material and 3 additional copies to the LIC for each solution as per the scope of work of the LIC. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.
vii. All out of pocket expenses related to training shall be borne by the selected bidder.
viii. The vendor may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training.

The detailed training documents should be given to the training participants. The detailed theory & hands-on training should be imparted by the OEM Authorized personnel at LIC premises.
The training facilities shall be made available by LIC, the Bidder will have to ensure that training is imparted in a professional manner through certified and experienced personnel (other than on-site Personnel) and proper courseware is given to every person attending the training.

G. Support Process Requirement:

i. The vendor shall provide an escalation matrix in consultation with the IT/BPR Department, Central Office, LIC for different categories of support calls.
ii. Day-to-day maintenance of the complete solution setups made.
iii. The support Personnel provided should be conversant with the regular configuration from scratch, integration with other log sources, creation of rules and policies as per LICs requirements, administration tasks, patch management, user management, backup procedures, etc.
iv. The on-site support Personnel should be able to troubleshoot the problems raised and should maintain a log of them, also report it to the LIC administrators in detail with root cause analysis and problem resolution.
v. The Bidder should ensure that there will be a proper change & configuration management, backup management, security management. These procedures should be well documented, followed and maintained (copy of the same should be submitted to LIC Central Office – IT dept.)
vi. The onsite support Personnel should re-install/ reconfigure any component/ system of the security equipment supplied by the vendor, in case of crash of those components / system on problem or patch/upgrades. The on-site Support Personnel also needs to support, if any security installations done by a separate vendor.
vii. In case the problem is not being rectified by the onsite L1 & L2 Personnel even after 1 hour, the issue should be escalated and resolved within 4 hr. from time of incident.
viii. The support Personnel should also keep track of the issues /ticket raised through the web interface help desk/telephone/mail etc. and should provide the solution for the same.
ix. There should be a provision to audit the changes done to fix the accountability.
x. Up gradation of products to the latest version at all the locations, whenever applicable by following a risk-based approach. The procedures have to be documented and submitted to LIC before carrying out any such activity.
xi. The vendor has to do necessary implementations required from business continuity perspectives with respect to all the solutions.
xii. Root cause analysis of any event has to be done and proper corrective action has to be taken with information to LIC officials. Based on that, the vendor should recommend for improvement to policies, procedures, tools, and other aspects.

xiii. 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.

xiv. Alert LIC officials for any unusual occurrence/threat/attacks etc. observed.

o. The vendor has to comply with the following attributes related to all the in-scope solutions:

- LIC has a right to review their processes
- SOPs for the processes.
- LIC has a right to assess the skill sets of vendor resources.
- Advance information about the resources deployed is to be communicated and proper hand-over of charge with complete documentation has to be done for the new resources, which should be approved by LIC.
- All necessary steps/changes have to be made in security infrastructure as per the requirements of ISO27001, Certifying Authority/ Body etc. or any third-party security audit / inspection report.

Note:

- No telephone connection will be provided by LIC to the onsite support persons.
- The on-site L1 and L2 support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.

H. On-Site Support Services:

I. Cloud Access Security Broker (CASB)

- 8x5 real-time monitoring uptime, availability, health performance of CASB devices with mitigation support.
- Track and follow-ups with stake-holders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management
- Perform periodic review and fine tuning of these devices to fit organization network environment and requirement, subsequence management, monitoring and support (8x5)
- The change management of all the devices must be adhering to standards and policies of LIC.
- Create, update, and delete access control rules, groups, and policies in CASB after obtaining approval.
- Quarterly review of rules, policies etc. of applications and recommend optimization of the same.
- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the On-Site Support
- Quarterly review of capacity planning of SaaS based services. Details of underutilized and over utilized LIC SaaS based applications.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks

- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Maintain security product configuration, based on industry best practices, and as requested,
- Participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design
- Tracking/Alerting the required license, software subscription for all software components of devices in scope
- Set up and manage admin and user accounts. Perform access control as per need basis
- Conduct Recovery exercise of above points on quarterly basis or as per the LIC guidelines. Submit the Periodic Reports on the backup status
- On-Site Support should provide relevant support for external and internal security audits that LIC is subject to from time to time
- On-Site Support should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time

II. Network Access Control (NAC)

- 24x7 real-time monitoring, availability and health performance of NAC devices with mitigation support.
- Track and follow-ups with stakeholders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- Service Provider shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- The pre-requisites for onboarding all devices should be intimated to LIC well in advance of the onboarding process. It is bidder's responsibility to ensure that all pre-requisites are in place before the onboarding process starts. If the bidder faces any problem to ensure that the pre-requisites are in place the same should be intimated to LIC in writing as per LIC escalation matrix.
- Service Provider must ensure a smooth onboarding of all the devices. If Service Provider faces any problem, while onboarding the devices due to lack of certain pre-requisites the same must be assisted and intimated to LIC in advance.
- After onboarding if any issues are faced by any users the same has to be rectified as per SLA.
- If after the completion of onboarding process, any new device is added to the network or any existing device is replaced it is the vendor's responsibility in consultation with the LIC's team to ensure that all the necessary configurations are in this device for seamless integration with NAC else penalty as per SLA will be applicable. If the vendor faces any difficulties in fulfilling the obligations, owing to dependency on LIC the same has to be intimated in writing as per escalation matrix provided by LIC.
- Perform periodic review and fine tuning of these devices to fit organization network environment and requirement, subsequent management, monitoring and support (24x7)
- The change management of all the devices must be adhering to standards and policies of LIC.
- Create, update, and delete access control rules, groups, and policies in NAC after obtaining approval.
- Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.
- For the VVIP (ED and above) users tolerance level will be zero.

- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the Service Provider
- Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- 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
- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Maintain security product configuration, based on industry best practices, and as requested,
  participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design
- Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
- Set up and manage admin and user accounts. Perform access control as per need basis
- Conduct quarterly recovery exercises for in-scope solution in accordance with LIC guidelines and submit periodic reports detailing the status of the backup exercises.
- Service Provider should provide relevant support for external and internal security audits that LIC is subject to from time to time
- Service Provider should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time
- Any services related to the solution which may be send by the LIC from time to time.

III. SSL Off loader

- 24x7 real-time monitoring uptime, availability, health performance of SLL Off loader devices with mitigation support.
- Track and follow-ups with stakeholders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- The SSL Off loader in a WAF should be from different OEM.
- On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management
- Perform periodic review and fine tuning of these devices to fit organization network environment and requirement, subsequence management, monitoring and support (24x7)
- The change management of all the devices must be adhering to standards and policies of LIC.
- Create, update, and delete access control rules, groups, and policies in SSL Off loader after obtaining approval.
- Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.

- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the On-Site Support.
- Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- Any services related to the solution which may be send by the LIC from time to time.
- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Maintain security product configuration, based on industry best practices, and as requested,
- Participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design
- Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
- Set up and manage admin and user accounts. Perform access control need basis
- Conduct quarterly recovery exercises for in-scope solution in accordance with LIC guidelines and submit periodic reports detailing the status of the backup exercises.
- On-Site Support should provide relevant support for external and internal security audits that LIC is subject to from time to time
- On-Site Support should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time

IV. Web Application Firewall (WAF)

- 24x7 real-time monitoring uptime, availability, health performance of WAF devices with mitigation support.
- Track and follow-ups with stakeholders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management.
- The change management of all the devices must be adhering to standards and policies of LIC.
- Create, update, and delete access control rules, groups, and policies in WAF after obtaining approval.
- Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.
- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the On-Site Support.
- Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis

- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Any services related to the solution which may be send by the LIC from time to time.
- Maintain security product configuration, based on industry best practices, and as requested,
  participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design
- Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
- Set up and manage admin and user accounts. Perform access control need basis
- Conduct quarterly recovery exercises for in-scope solution in accordance with LIC guidelines and submit periodic reports detailing the status of the backup exercises.
- On-Site Support should provide relevant support for external and internal security audits that LIC is subject to from time to time
- On-Site Support should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time

V. Virtual Desktop Infrastructure (VDI)

- 24X7 real-time monitoring uptime, availability, health performance of VDI devices with mitigation support.
- Track and follow-ups with stake-holders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management.
- Perform periodic review and fine tuning of these devices to fit organization network environment and requirement, subsequence management, monitoring and support (8x5)
- The change management of all the devices must be adhering to standards and policies of LIC.
- Create, update, and delete access control rules, groups, and policies in WAF after obtaining approval.
- Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.
- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the On-Site Support.
- Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- Any services related to the solution which may be send by the LIC from time to time.

- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Maintain security product configuration, based on industry best practices, and as requested,
  participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design
- Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
- Set up and manage admin and user accounts. Perform access control need basis
- Conduct quarterly recovery exercises for in-scope solution in accordance with LIC guidelines and submit periodic reports detailing the status of the backup exercises.
- On-Site Support should provide relevant support for external and internal security audits that LIC is subject to from time to time
- On-Site Support should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time

VI. Mobile Device Management (MDM)

- Track and follow-ups with stake-holders for resolution of reported incidents tickets.
- Ensure systems are up and running, including their other aspects like Configuration, Re-configuration, updates, upgrades, bug fixes, problem analysis, performance analysis, configuration optimizations, migration of devices, audits, users profile management, root cause analysis, on-site support.
- On-Site Support shall ensure logical and acceptable conclusion of all the monitoring, management, mitigation, administration, and reporting issues.
- On-Site Support must ensure a smooth handover of these devices from current vendor in specified and declared timelines with proper project management.
- The change management of all the devices must be adhering to standards and policies of LIC.
- Quarterly review of rules, policies etc. of security devices and recommend optimization of the same.
- Any services related to the solution which may be send by the LIC from time to time.
- SOP Documentation and OEM/Service Provider SLA management must be reviewed, implemented, and finetuned by the On-Site Support.
- Quarterly review of capacity planning of security devices. Details of underutilized and over utilized security devices.
- Open a case with OEM /product support for all faults. Coordinate with OEM /product support for resolution. Communicate status to LIC on a regular basis
- Provide recommendations for architecture enhancements/changes that can enhance the security posture
- Management of the security products for policy changes including rule changes, signature updates arising from business requirements or in the event of attacks
- Provide LIC with a root cause analysis of downtime due to faults, security events including preventive measures being taken to prevent future similar incidents and outages
- Maintain security product configuration, based on industry best practices, and as requested,
  participate in technical and business planning sessions to establish security standards, architecture, and project initiatives where the security products may impact or improvise the design

- Tracking/Alerting the required license, software subscription for all hardware & software components of devices in scope
- Set up and manage admin and user accounts. Perform access control need basis
- Conduct quarterly recovery exercises for in-scope solution in accordance with LIC guidelines and submit periodic reports detailing the status of the backup exercises.
- On-Site Support should provide relevant support for external and internal security audits that LIC is subject to from time to time
- On-Site Support should support POCs or evaluation of new technologies or tools relevant to services within this RFP from time to time.

2. Detailed Scope of Work

I. General Requirements

i. The specifications given are minimum. Bidders can quote equivalent or higher technical specifications to meet the requirements of LIC. The RFP and annexures together constitute the overall requirements of the solution.

ii. The bidder / System Integrator shall engage the services of respective OEMs/OEM certified partners 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.

iii. 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 modelling and predictive analysis capabilities of the solution for detection of threats for enhanced protection of LIC's infrastructure during the tenure of this project.

iv. 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.

v. 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.

vi. The bidder is responsible for the AMC, licenses, uptime, availability, and management of the devices/solutions implemented and managed as part of the in-scope solutions.

vii. The bidder shall Supply, Design, Install, Implement, Integrate, Support & Maintain all the in-scope solutions within this RFP.

viii. The bidder should consider the detailed technical specifications as stated in the Annexure E while proposing for the solution. Bidder needs to provide complete end to end solution including applicable appliances, software, necessary accessories, active and passive components for efficient functioning of the proposed solution.

ix. The bidder should provide backup solution for proposed setup. The backup taken should be SHA-256 encrypted. This backup refers to the configuration backup for the solutions provided by the bidder. The backup should be taken daily. The backup should be stored in the server in DC, and a replicated copy to be saved at the DR. Any configuration at DC should be replicated to DR on a real time basis. Additionally, it is essential that backups for the past 30 days remain accessible on a daily basis.

x. Bidder has to quote for highest/ premium support available from the OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs.

xi. The bidder and OEM/OEM certified partner 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:

i. Solution architecture, sizing, policy configuration, High availability, BCP/ DR scenarios, etc.
ii. Integration of each solution with other in scope solutions and other Network and Security solutions currently deployed in the environment as decided by the LIC.
iii. Testing strategy and test cases for Acceptance Testing of the solution.
iv. Identifying gaps, crown jewels of LIC, custom parser creation, creation of rules, use case development, finetuning, etc.

xii. The bidder and OEM/OEM certified partner shall submit a Requirement Gathering Document and a detailed Design Document based on the requirements gathering exercise.

xiii. All the solutions should be seamlessly integrated with the LIC's NTP solution and must be compatible with any provided NTP version.

xiv. In case there is a cost incurred to LIC due the wrong BoM/Specification/feature-set of security equipment/device/appliance at any location, the same will have to be replaced by vendor at no extra cost to LIC.

xv. Prepare test-plan, implementation plan, integration plans and rollback strategies.

xvi. 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.

xvii. The successful bidder needs to install all the associated equipment needed to complete the job as per the technical specification described in this tender.

xviii. The successful bidder shall co-ordinate and co-operate with the other vendors appointed by the LIC so that the work shall proceed smoothly without any delay and to the satisfaction of LIC.

xix. No extra claim shall be entertained on account of all/part of any job redone on account of bidder's negligence which results into damages/losses during execution of the job. Also, any component(s) required to deliver the solution after release of Purchase Order shall have to be provided by the successful bidder. All such cost shall be borne by the bidder.

xx. The vendor has to provide complete escalation matrix which should be updated and sent to LIC as and when there is a change.

xxi. Bidder has to architect the solution deployment after understanding the following details:

- Understanding the environment in terms of application, network, server and Security appliances, LAN, WAN & Internet Links and segments, privileged users etc. to ensure creation of use cases related to targeted attacks and early breach detection.
- Prepare the designs and implement the solution in line with IRDAI's guidelines on Information and cyber security for Insurers, ISO27001:2013/ISO22301/IT Act 2001 (along with its amendments) standards as modified from time to time. Study of LIC's existing security and application environment and guidelines and recommend best practices to implement and roll out the same.
- To suggest plan for network integration of various devices/appliances etc. with the proposed solutions. Design of the proposed solutions.
- Integration and co-ordination within scope solutions in future.
- Bidder needs to prepare a detailed execution plan. The complete documented plan must be submitted to LIC with supported designs and drawings (if any) within 5 weeks of placing the order. The actual execution will start only after approval of plan by LIC officials.
- The plan shall include information related to required downtime, changes to existing architecture, log level parameters, deployment schedule etc.
- The installation of the appliances shall be done as a planned activity on a date & time of approved deployment schedule.

xxii. 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.

II. Cloud Access Security Broker (CASB)

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.
ii. The vendor should configure CASB for guaranteeing the secure and regulatory-compliant utilization of cloud services.
iii. The vendor must provide the solution that must be compliant with GDPR, DPDP, IRDAI.
iv. The vendor must encompass enforcing security policies, safeguarding sensitive data, overseeing user access, monitoring cloud operations, ensuring adherence to regulations, and mitigating potential cybersecurity risks.
v. The vendor should provide services including data loss prevention (DLP), threat detection, encryption, access control, and compliance monitoring.
vi. The vendor must provide the solution that must be compatible with existing cloud infrastructure, including AWS and Azure, and support seamless integration with the Single Sign-On (SSO) system.
vii. The vendor must assist in achieving and maintaining compliance with industry regulations, including HIPAA, and should offer comprehensive reporting for audit purposes.
viii. The vendor must provide the solution that should be deployed both in proxy and API modes and seamlessly integrate with cloud-based services like Office 365, Salesforce, and Dropbox.
ix. The vendor must deploy the solution seamlessly and integrate with cloud-based managed services.
x. The vendor should manage user authentication, provide role-based access control, and apply encryption to sensitive data, both at rest and in transit.
xi. The vendor must offer advanced threat detection capabilities, with automated incident response and alerting mechanisms.
xii. The vendor must offer detailed logging of user activities and security events. Real-time monitoring should be available through a user-friendly dashboard.
xiii. The vendor should support encryption using industry-standard protocols and provide granular data loss prevention policies to protect intellectual property.
xiv. The vendor should offer on-site and remote training for administrators and end-users, as well as remote 8x5 technical support with on-call if required.
xv. Onsite L3 support is required by LIC during the implementation phase and once the sign-off is provided by LIC the support of L3 will not be further required.
xvi. The vendor should be able to scale to accommodate our growing user base and cloud usage while maintaining high performance.
xvii. The vendor shall enable a CASB self service portal for LIC stakeholders to review, monitor and administer the service request.

III. Network Access Control (NAC)

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.
ii. Bidder should propose a Load Balancer required for implementation of the NAC Solution. This Load Balancer will be different from the Server Load Balancer (SLB) included in scope of this RFP.
iii. The vendor should deploy NAC within the organization's network.
iv. The vendor must enforce security policies, profiling, posturing, guest-portal, sponsor portal, monitor, and control network access, and protect against unauthorized devices and threats.
v. The vendor should provide services including user authentication, device profiling, device posturing, policy enforcement, and threat detection.

vi. The vendor must provide the solution that must be compatible with our network infrastructure, supporting integration with our existing switches, routers, and firewalls.
vii. The vendor should assist in achieving and maintaining compliance with regulatory standards such as PCI DSS and provide reporting for audit purposes.
viii. The vendor should deploy the solution across our network and integrate seamlessly with directory services, such as Active Directory, for user authentication.
ix. The vendor should manage user authentication, device identification, and ensure that only authorized and compliant devices gain network access.
x. The vendor must offer advanced threat detection capabilities, with automated incident response and alerting mechanisms.
xi. The vendor should provide detailed logging of user and device activities and real-time monitoring through a centralized dashboard.
xii. The vendor should enforce security policies and support automated or manual remediation actions for non-compliant devices.
xiii. The vendor should offer on-site and remote training for administrators and 8x5 technical support for issue resolution.
xiv. Onsite L3 support is required by LIC during the implementation phase once the sign-off is provided by LIC the support of L3 will not be further required.
xv. The solution should scale to accommodate our network growth and maintain high performance, even during peak usage.
xvi. Any other function/configuration/job required for smooth functioning of the solution/entire setup.

IV. SSL Off loader

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.
ii. The vendor should deploy SSL Off loader within the organization's network.
iii. The vendor should enhance the performance of web services by offloading SSL/TLS encryption and decryption from the backend servers.
iv. The vendor should be able to provide load balancing capabilities to distribute client requests among multiple backend servers
v. The vendor should ensure the security and privacy of data transmitted over SSL/TLS connections.
vi. The vendor should optimize SSL/TLS certificate management and improve network efficiency.
vii. The vendor should implement load balancing and traffic management settings.
viii. The vendor should verify the SSL Off loader's functionality and connectivity.
ix. The vendor should perform security and performance testing to validate the system's effectiveness.
x. The vendor should resolve any issues or discrepancies identified during testing
xi. Onsite L3 support is required by LIC during the implementation phase once the sign-off is provided by LIC the support of L3 will not be further required.
xii. The vendor should provide the solution that is scalable to accommodate traffic spikes and maintain high performance under heavy loads.
xiii. Any other function/configuration/job required for smooth functioning of the solution/entire setup.
xiv. Proposed SSL off loader and WAF should not be from same OEM.

V. Web Application Firewall (WAF)

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.

ii. The vendor should deploy WAF within the organization's network.
iii. The vendor should provide services such as application-layer attack detection and mitigation, DDoS protection, and real-time threat monitoring.
iv. The vendor must provide the solution that must be compatible with our web application stack, including support for popular web servers and content management systems.
v. The vendor should assist in achieving and maintaining compliance with industry standards, such as PCI DSS, and provide detailed reporting for audit purposes.
vi. The vendor should deploy the solution in-line with our web application infrastructure and integrate seamlessly.
vii. Onsite L3 support is required by LIC during the implementation phase once the sign-off is provided by LIC the support of L3 will not be further required.
viii. The vendor should provide the solution that offer real-time attack detection and mitigation for SQL injection, cross-site scripting (XSS), and other application-layer threats.
ix. The vendor must provide the solution that support rate limiting to mitigate brute force and other abusive behaviors and provide bot protection mechanisms.
x. The vendor must provide solution that should maintain detailed logs of traffic and security events and offer a user-friendly dashboard for real-time monitoring.
xi. The vendor must provide solution that should support content delivery, caching, and SSL termination to improve web application performance while maintaining security.
xii. The vendor should provide the solution that should be scalable to accommodate traffic spikes and maintain high performance under heavy loads.
xiii. Any other function/configuration/job required for smooth functioning of the solution/entire setup.
xiv. Proposed SSL off loader and WAF should not be from same OEM.

VI. Virtual Desktop Interface (VDI)

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.
ii. The vendor should deploy VDI solution within the organization's network.
iii. The vendor should provide proposed solution that should be able to deliver desktops/applications to the end user by providing dedicated OS per user and by sharing the Operating System resources on the Server.
iv. The vendor should provide the solution that must be compatible with our web application stack, including support for popular web servers and content management systems.
v. The vendor should provide the solution that should assist in achieving and maintaining compliance with industry standards, such as PCI DSS, and provide detailed reporting for audit purposes.
vi. The vendor should provide the solution that should be deployed in-line with our web application infrastructure and integrate seamlessly.
vii. The vendor should offer on-site and remote training for administrators and 24X7 technical support for issue resolution.
viii. The vendor must support Windows based desktop virtualization with the ability to run Windows 7, 8.1, Windows 10 and Windows 11 OS
ix. The vendor must support Windows session based desktop virtualization on windows server operating system with support for Windows Server 2012R2, Windows 2016 and Windows Server 2019.
x. The vendor must support Application virtualization on windows server operating systems with support for Windows 2012R2, Windows 2016 and Windows Server 2019
xi. The vendor must support Linux based desktop virtualization with support for RHEL, Ubuntu and CentOS distributions.

xii. The vendor must support shared virtual desktops based on Linux terminal services with support for RHEL, Ubuntu and CentOS distributions.
xiii. The vendor must support multiple users sharing single Windows & Linux Server in case of Server OS based application virtualization.
xiv. The vendor should secure the data within datacenter unless allowed by administrator based on policy.
xv. The vendor must support persistent and non-persistent virtual desktops.
xvi. The vendor must support time bound provisioning and de-provisioning of virtual desktops.
xvii. The vendor must provide proposed solution that shall provide access to desktops and / or applications via one of the commonly used remote access protocols like HDX/ICA/PCOIP/BLAST Extreme/RDP/RemoteFX
xviii. The vendor must provide solution that shall have multi-tenant function to support creation of multiple organizations with their own authentication server, resources, applications and administrative domains.
xix. Fingerprint Biometric authentication support for business application even in shared hosted desktop using Windows end point.
xx. The vendor must be ready to customize product in case any regulatory compliances change/enforced during contract period to safeguard the investment.
xxi. The vendor must have API for seamless integration with internal applications such as Active Directory, Microsoft O365, Core Insurance Application of LIC, HRMS, Windows Login, Wi-Fi Controllers, RADIUS, Network Devices, Linux Logon, Headless server logon etc without any additional cost.
xxii. Any other function/configuration/job required for smooth functioning of the solution/entire setup.

VII. Mobile Device Management (MDM)

i. The vendor should assess the existing security infrastructure and identify any gaps or vulnerabilities.
ii. The vendor should assist in achieving and maintaining compliance with industry standards, such as PCI DSS, and provide detailed reporting for audit purposes.
iii. The vendor must provide the solution that should be deployed in-line with our web application infrastructure and integrate seamlessly.
iv. The vendor should offer on-site and remote training for administrators and 24X7 technical support for issue resolution.
v. The vendor must provide the solution that should allow seamless integration of existing technology/application systems and establish technology platform for future enterprise integrations.
vi. The vendor should envisage outlined indicative functionalities for the proposed EMM solution: Support BYOD (employee devices) and corporate devices, Containerization to separate private and business data.
vii. The vendor should support the outlined applications inside the container: Secured email, container application, selected mobility applications.
viii. The vendor must provide the solution that should be capable of:
    - Blocking corporate e-mail attachments, business files sharing through third party un-authorized applications like Gmail, SHAREIt, etc., Bluetooth, OTG, Wi-Fi, LAN or any other File-sharing mechanisms
    - Applying or modifying default device policy settings
    - Creating and distributing customized acceptable-use policies
    - Defining role-based administrative portal access rights for administrators
    - Approving or quarantining new mobile devices on the network

- Monitoring devices
- Selectively wiping corporate data leaving personal data intact
- Managing patches and updates
- Managing identities (Role-based policies through Active Directory)
- De-commissioning of devices by removing corporate data and UEM/EMM control
- Managing user mail profile
- Enforcing encryption and password visibility settings
- Implementing real-time compliance rules with automated actions
- Configuring passcode policies using quality, length and duration
- Sending notification to devices
- Making provision of self-service portals
- Detect and restrict jailbroken and rooted devices
- Rogue Device Access Revocation
- Simple Device Enrollment

ix. The vendor should be capable of instant discovery of devices accessing enterprise systems, connect with other operational systems through robust web APIs.

x. Any other function/configuration/job required for smooth functioning of the solution/entire setup.

VIII. Server Load Balancer (SLB)

i. Supply of SLB with provision for version upgrades/patches.

ii. Installation and implementation as per the agreed network & security architecture design; this will include rules/policy definition and enforcement on the devices proposed in this RFP.

iii. Vendor has to act as technical advisor to LIC for SLB and related systems by way of evaluation, demonstration, etc. as and when required by LIC.

iv. Identification of potential security risks and helping LIC to take appropriate corrective action.

v. Designing and implementing the proposed solution including migration of all the existing configuration and policies.

vi. Configuration and enablement of the licensed features wherever required by LIC.

vii. Implementation of new configuration and policies, wherever required.

viii. Preparation of test-plan, migration plan and rollback strategies.

ix. The successful bidder shall coordinate and cooperate with existing vendors appointed by LIC wherever required.

x. Any other function/configuration/job required for smooth functioning of the solution/entire setup.

3. Sizing Requirements

SN	Solution	Sizing	DC	DR	NDR
1	Cloud Access Security Broker (CASB)	100 Roaming Users	Single Setup	-	-
2	Network Access Control (NAC)	As per Technical specifications	Active along with Load Balancer in HA for this solution	Passive along with required Load Balancer for this solution	-
3	SSL Offloader	As per Technical specifications	HA (1+1)	HA (1+1)	HA (1+1)
4	Web Application Firewall (WAF)	As per Technical specifications	HA (1+1)	HA (1+1)	HA (1+1)

SN	Solution	Sizing	DC	DR	NDR
5	Mobile Device Management (MDM)	100000 devices	HA (1+1)	HA (1+1)	-
6	Virtual Desktop Interface (VDI)	800 Users	Single Setup	Single Setup	-
7	Server Load Balancer (SLB)	As per Technical specifications	HA (1+1)	HA (1+1)	HA (1+1)

4. RACI Matrix

Below Table depicts desired RACI (Responsible-R, Accountable-A, Consulted-C, Informed-I) matrix for in-scope solutions which is non-exhaustive. The successful bidder must submit comprehensive RACI for proposed services in a similar way in their response to RFP.

SN	Service	Activity	SI	OEM/OEM Certified Partner wherever applicable	LIC
1	Cloud Access Security Broker (CASB)	Plan, Design, Implementation	R, A	R, A	C, I
		Service Request Handling	R, A	C	I
		Problem Management- Root Cause Analysis	R, A	R, A	C, I
		Configuration Change Plan	R, A	C	I
		Inventory Management	R, A	C	I
		License Management	R, A	C	I
		SLA Performance	R, A	R, A	C, I
		SLA Reporting	R, A	C	I
		Service Delivery Review and Governance	R, A	R, A	C, I
		Business Continuity Management	R, A	R, A	C, I
2	Network Access Control (NAC)	Plan, Design, Implementation	R, A	R,A,C	I
		Service Request Handling	R, A	C	C, I
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	C	C, I
		Software Implementation	R, A	R, A, C	C, I
		Inventory Management	R, A	C	I
		License Management	R, A	C	C, I
		SLA Performance	R, A	C, I	C, I
		SLA Reporting	R, C	R	A, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I
3	SSL Off loader	Plan, Design, Implementation	R, A	R, A, C	I
		Service Request Handling	R, A	I	C, I
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	C	C, I
		Software Implementation	R, A	R, A, C	C, I

SN	Service	Activity	SI	OEM/OEM Certified Partner wherever applicable	LIC
		Inventory Management	R, A	C	I
		License Management	R, A	C	C I
		SLA Performance	R A	C, I	C, I
		SLA Reporting	R, C	R	A, I
		Assess impact of incidents	R, A	I	C, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I
4	Web Application Firewall	Plan, Design, Implementation	R, A	R A C	I
		Service Request Handling	R, A	I	C I
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	C	C, I
		Software Implementation	R, A	R, A, C	C, I
		Inventory Management	R, A	C	I
		License Management	R, A	C	C I
		SLA Performance	R, A	C, I	C, I
		SLA Reporting	R, C	R	A, I
		Assess impact of incidents	R, A	I	C, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I
5	Virtual Desktop Interface (VDI)	Plan, Design, Implementation	R, A	C	I
		Service Request Handling	R, A	I	C
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	I	C, I
		Software Implementation	R, A	R	C, I
		Inventory Management	R, A	C	I
		License Management	R, A	C	I
		SLA Performance	R	A	C, I
		SLA Reporting	R, C	R	A, I
		Assess impact of incidents	R, A	I	C, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I
6	Mobile Device Management (MDM)	Plan, Design, Implementation	R, A	R A C	I
		Service Request Handling	R, A	I	C
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	C	C, I
		Software Implementation	R, A	R, A, C	C, I
		Inventory Management	R, A	C	I
		License Management	R, A	C	C, I

SN	Service	Activity	SI	OEM/OEM Certified Partner wherever applicable	LIC
		SLA Performance	R, A	C, I	C, I
		SLA Reporting	R, C	R	A, I
		Assess impact of incidents	R, A	I	C, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I
7	Server Load Balancer (SLB)	Plan, Design, Implementation	R, A	C	I
		Service Request Handling	R, A	I	C
		Problem Management- Root Cause Analysis	R, A	C	I
		Configuration Change Plan	R, A	I	C, I
		Software Implementation	R, A	R	C, I
		Inventory Management	R, A	C	I
		License Management	R, A	C	I
		SLA Performance	R	A	C, I
		SLA Reporting	R, C	R	A, I
		Assess impact of incidents	R, A	I	C, I
		Threat modelling	R, A	A, I	C, I
		Validate CIA to assets in SIEM	R, A	I	C, I

5. Resource Deployment

Bidder shall deploy qualified resources with valid certification and relevant experience for conducting the in-scope activities at LIC Premises.

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
1	Service-Delivery Manager (SDM)/ Project Coordinator	• Develop a comprehensive project plan, including objectives, timelines, and resource requirements. • Establish effective communication channels and maintain positive relationships with stakeholders. • Identify and mitigate project risks, both technical and non-technical. • Efficiently allocate project resources, including personnel and budget.	L3	1	General Shift (8x5)	10 Years	PMP/ PRINCE2

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		• Maintain accurate project documentation, including technical specifications. • Ensure project deliverables meet established quality standards.					
2	CASB Security Analyst	• Gather information from all available, network diagrams, network architecture and design documentation. • Understand existing technology, process, organization estate and tailor-made questionnaire framework. • Understand the list of features enabled on the CASB solutions. • The L1 resource shall be utilized in a shared mode from the network resource deployment.	L1	1	8x5	3 Years	CEH
3	Network Access Control (NAC)	• Detailed plan for deployment • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Plan how to Integrate NAC data with SIEM. • Use cases to be configured (Compliance & Security related) • Define authorization mechanisms for granting access based on user roles and compliance requirements. • Plan the authentication methods for users and devices • Design where policy enforcement points will be located in the	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/ At least one NAC OEM related certifications

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		network. • Deploy the solution according to the defined plan and configuration requirements					
		• Gather information from all available, network diagrams, network architecture and design documentation • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Identify the network segments and access points that need to be controlled. • Understand the types of users and devices accessing the network. • Analyse the diversity of devices, operating systems, and security postures. • Assess the existing security measures, such as authentication methods and intrusion detection systems. • Identify vulnerabilities, potential attack vectors, and areas of weakness.	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any NAC solution
4	SSL Off loader (SSLO)	• Identify critical web applications that require protection. • Analyse application architecture, functionality, and potential security vulnerabilities • Evaluate historical and potential threats targeting web applications. • Understand attack patterns, attack vectors • Use cases to be configured (Compliance	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/ At least one SSL Off loader OEM related certifications

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		& Security related) • Define rule sets for blocking common web application attacks. • Plan how traffic will be routed through the SSL Off loader. • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Deploy the solution according to the defined plan and configuration requirements					
		• Identify critical applications that require protection. • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Analyse application architecture, functionality, and potential security vulnerabilities • Evaluate historical and potential threats targeting web applications. • Understand attack patterns, attack vectors, and potential impact. • Identify existing security measures and potential gaps in application protection. • Determine areas susceptible to attacks such as SQL injection, cross-site scripting (XSS), and more	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any SSLO solution
5	Web Application Firewall (WAF)	• Identify critical web applications that require protection. • Analyse application architecture,	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		functionality, and potential security vulnerabilities • Evaluate historical and potential threats targeting web applications. • Understand attack patterns, attack vectors • Use cases to be configured (Compliance & Security related) • Define rule sets for blocking common web application attacks. • Plan how traffic will be routed through the WAF. • Deploy the solution according to the defined plan and configuration requirements					At least one WAF OEM related certifications
		• Identify critical web applications that require protection. • Analyse application architecture, functionality, and potential security vulnerabilities • Evaluate historical and potential threats targeting web applications. • Understand attack patterns, attack vectors, and potential impact. • Identify existing security measures and potential gaps in application protection. • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Determine areas susceptible to attacks such as SQL injection, cross-site scripting	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any WAF solution

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		(XSS), and more					
6	Mobile Device Management (MDM)	• Detailed plan for deployment • Plan how to Integrate MDM data with SIEM and other security solutions. • Use cases to be configured (Compliance & Security related) • Define authorization mechanisms for granting access based on user roles and compliance requirements. • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Plan the authentication methods for users and devices • Design where policy enforcement points will be located in the network. • Deploy the solution according to the defined plan and configuration requirements	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/ At least one MDM OEM related certifications
		• Gather information from all available, network diagrams, network architecture and design documentation • Identify the network segments and access points that need to be controlled. • Understand the types of users and devices accessing the network. • Analyse the diversity of devices, operating systems, and security postures. • Assess the existing	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any MDM solution

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		security measures, such as authentication methods and intrusion detection systems. • Identify vulnerabilities, potential attack vectors, and areas of weakness.					
7	Virtual Desktop Interface (VDI)	• Detailed plan for deployment • Plan how to Integrate VDI data with SIEM and other security solutions. • Use cases to be configured (Compliance & Security related) • Define authorization mechanisms for granting access based on user roles and compliance requirements. • Liaise with the end users, in consultation with the LIC, for resolution of end users problems • Plan the authentication methods for users and devices • Design where policy enforcement points will be located in the network. • Deploy the solution according to the defined plan and configuration requirements	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/ At least one VDI OEM related certifications
		• Gather information from all available, network diagrams, network architecture and design documentation • Identify the network segments and access points that need to be controlled. • Understand the types of users and devices accessing the network. • Analyse the diversity of	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any VDI solution

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		devices, operating systems, and security postures. • Assess the existing security measures, such as authentication methods and intrusion detection systems. • Identify vulnerabilities, potential attack vectors, and areas of weakness.					
8	Server Load Balancer (SLB)	• Configure load balancer settings according to network requirements. • Manage virtual servers, server pools, and SSL certificates • Monitor server health and network traffic. • Optimize load balancing algorithms for optimal performance. • Ensure compliance with security standards and protocols. • Diagnose and resolve load balancer issues promptly. • Collaborate with other IT teams for complex problem-solving. • Maintain accurate documentation of configurations and changes. • Generate regular reports on performance metrics and security incidents	L2	1	8x5	5 Years	CEH/ CISSP/ CISM/ CCNP/ Any network security certification/ At least one SLB OEM related certifications
		• Assist with IP address setup and software installations. • Monitor alerts and escalate critical issues to L2 resources. • Perform routine maintenance tasks and basic technical support. • Update documentation related to system configurations and	L1	1	8x5	3 Years	CEH/ CCNA certified with experience of working on any SLB solution

SN	Resource	Responsibilities	Category	Count	Shift	Experience	Certifications
		procedures.					

Note:

a. The provision of on-site support is required in Mumbai.
b. To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored –
    - L1 Resource – Rs. 7 Lakhs per year.
    - L2 Resource - Rs. 9 Lakhs per year.
    - L3 Resource - Rs. 14 Lakhs per year.

    Note: The minimum compensation for the resources shall be at least as per the above figures. LIC reserves the right to verify the same.
c. LIC will conduct interviews of the proposed resources in-scope solutions. It reserves the right to reject any resource which is not suitable for the proposed role.
d. All the deployed resources will be monitored based on their skills and performance for the initial six months of the project. In case the performance of the deployed resources is not up to the mark during this period, LIC reserves the right to replace such resources. In this case, the Bidder has to onboard suitable resource with relevant skillset at no additional cost to the LIC.
e. In case of exigencies, or as and when required by the LIC the onsite resources should be available on Sundays and Public Holidays as well.

Onsite Support Services:

The successful Bidder has to provide throughout the contract period, the services of an onsite L1 & L2 support personnel at Central office (IT), Mumbai with the qualifications and experience as described below. As per the changing business needs, LIC may ask the Personnel to report for duty in different Time Windows as per the need of LIC.
The successful bidder has to submit a Background Verification Report conducted by Police of all resources deployed (L1 support, L2 support, and Service Delivery Manager)

L1 onsite support personnel Qualifications:

a. Should have good knowledge on implementation and its functionality of security products in a heterogeneous environment
b. Should be in the pay-roll of the vendor i.e. not outsourced.
c. For seamless integration of the entire solution, the onsite support will have to co-ordinate with the various projects and resolve the problem.
d. The L1 should have a backup resource of L2 who will complement the person during routine jobs and supplement, if he is on leave. The L2 should be accountable for the providing the technical support to LIC.
e. The L1 should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.
f. He should have the competency to educate the Security administrators of LIC at Central office with regard to daily jobs; trouble- shoot any related issues etc.
g. If the performance is not up to the mark, the Personnel may have to be changed, if LIC so requests.

L2 onsite support personnel Qualifications:

a. Should have good knowledge on implementation and its functionality of security products in a heterogeneous environment.

b. Should be able to do day-to-day maintenance of all security devices/appliances/equipment etc. at all locations.
c. Should help to locate issues related to security aspects and notify the same and assist in its resolution.
d. Should be able to do required changes in configuration, policies, etc.
e. Should be in the pay-roll of the vendor i.e. not outsourced.
f. For seamless integration of the entire solution, the vendor will have to co-ordinate with the various projects and resolve the problem.
g. The L2 should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.
h. The person should have a backup resource of L2 / L3 who will complement the person during routine jobs and supplement, if he is on leave. The L2 / L3 should be accountable for providing the technical support to LIC.
i. He should have the competency to educate the Security administrators of LIC at Central office with regard to daily jobs; trouble- shoot any related issues etc.
j. If the performance is not up to the mark, the Personnel may have to be changed, if LIC so requests.

Following conditions shall be applicable regarding the onsite L1/L2 support:

i. All the onsite support candidates should be dedicated resources to LIC.
ii. Details of the concerned candidates along with his/her Curriculum Vitae (CV) are to be provided to LIC along with the photo-identity and supporting documents (duly verified and attested by vendor) within 5 weeks from the date of issue of purchase order/Letter-of-Intent.
iii. If required, the candidates (for onsite support at LIC) may be interviewed by LIC officials or LIC's consultant or persons nominated by LIC; including hands on troubleshooting etc. based on which the candidate will be assessed and shortlisted.
iv. If the candidate is not found to be suitable, vendor will have to provide an alternate candidate. The selected candidate has to report to the LIC, within 2 weeks of being intimated of the selection by LIC.
v. Shortlisted candidates will also form a standby pool for LIC. Candidates from this pool only will be accepted by LIC for the onsite support (including the standby resource). In case of attrition/resignation, the pool has to be updated on regular basis following the process defined above.
vi. In case of a person going on leave, suitable replacement shall be provided from the pool for that leave-period failing which penalty as per the SLA conditions shall be applicable.
vii. If any on-site support person leaves before expiry of one year, penalty as per SLA conditions shall be applicable. This will be cumulative in nature for each occurrence.
viii. In case the on-site support person is to be changed by the vendor, minimum of one-and-half month (45 days) advance notice shall be given by the vendor to LIC, for reasons other than termination, death and hospitalization. On-site support person may have to be changed by the vendor, if LIC so desires. Notice period for the same will be of 30 days from LIC.
ix. The selected vendor will also have to earmark a Project Coordinator for LIC, who will act as the advisor/consultant for issues and may have to come for meeting at LIC and work on the new initiatives that LIC may take from time-to-time. No charges will be payable by LIC for this purpose. Project Coordinator should also coordinate with other teams/OEM for effective project delivery.
x. The vendor shall provide the background verification, including Police Clearance Report of the onsite resources.
xi. Overall monitoring, management, and Quality Service Delivery

xii. In-scope solution's equipment health monitoring.
xiii. Data Backup & Recovery
xiv. Software patches and updates as provided by the OEM from time to time
xv. Monitoring of ports, Rules, Change in Rules and its impact analysis
xvi. Periodic assessments, maintenance, and health audit of individual device as well as that of the overall infrastructure
xvii. Resolution of both logical and physical issues/ problems relating to the solution and/or related processes.
xviii. Maintain Device Configuration
xix. Crisis management and Emergency response procedures
xx. Real time visibility to resource utilization statistics
xxi. Ensure Managed Components can successfully send and receive and/or process data traffic and report failed passwords and community SNMP strings
xxii. Detect that an Event has occurred by monitoring syslog, SNMP trap messages, KPIs, and/or Threshold Crossing Alerts from Managed Components
xxiii. Proactive insights to help remediate issues quickly and also detailed drill-downs to identify the impact quickly.
xxiv. Maintain History of critical events
xxv. Plan & Validate critical changes and prepare Change Procedure, Analyze impact of Change and execute approved changes
xxvi. Verify software releases, bug fixes, vulnerability fixes and identify recommended software.
xxvii. Capacity and License Management
xxviii. Log Collection and Analysis
xxix. Root Cause Analysis for Critical & Repetitive Incidents
xxx. Preparation of frequently known error datasheet
xxxi. Support scheduled mocks and DR drills.
xxxii. Daily Checklist and Historical Trend Analysis
xxxiii. Manage the lifecycle of Change Management Requests, as required, resulting from an Incident, Problem, Service Request
xxxiv. Service Request, Change and Incident Tracker
xxxv. Audit and Compliance Readiness Support

SUPPORT PLAN: The Bidder should provide a detailed plan on the support for the Security solution to maintain the system uptime of at least 99.9%.

SUPPORT PROCESS REQUIREMENT:

a. The vendor shall provide an escalation matrix in consultation with the IT/BPR Department, Central Office, LIC for different categories of support calls.
b. Day-to-day maintenance of the setup provided under the scope of this RFP.
c. The support Personnel provided should be conversant with the regular Configuration from scratch, administration tasks, patch management, user management, backup procedures etc.
d. The on-site support Personnel should be able to troubleshoot problems raised and should maintain a log of them, also report it to the LIC administrators in detail with root cause analysis and problem resolution.
e. The Bidder should ensure that there will be a proper change & configuration management, backup management, security management. These procedures should be well documented, followed and maintained (copy of the same should be submitted to LIC Central Office – IT dept.)
f. The onsite support Personnel should re-install/ reconfigure any component/ system of the security equipment supplied by the vendor, in case of crash of those components /

system on problem or patch/upgrades. The on-site Support Personnel also needs to support, if any security installations done by a separate vendor.

g. In case the problem is not being rectified by the onsite L1 & L2 Personnel even after 1 hour, the issue should be escalated and resolved within 5Hrs from time of incident.
h. The support Personnel should also keep track of the issues /ticket raised through the web interface help desk/telephone/mail etc. and should provide the solution for the same.
i. 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.
j. Upgradation of products to the latest version at all the locations, whenever applicable by following a risk-based approach. The procedures have to be documented and submitted to LIC before carrying out any such activity.
k. The vendor has to do necessary implementations required from business continuity perspectives with respect to network gateway security.
l. Risk based approach has to be implemented for any change management effected in the configurations carried out in the Firewall, etc.
m. Root cause analysis of any event has to be done and proper corrective action has to be taken with information to LIC officials. Based on that, the vendor should recommend for improvement to policies, procedures, tools and other aspects.
n. Alert LIC officials for any unusual occurrence/threat/attacks etc. observed.
o. The vendor has to comply with the following attributes related to network gateway security:
    - LIC has a right to review their processes
    - SOPs for the processes in the 4 locations where deployment is done.
    - LIC has a right to assess the skill sets of vendor resources.
    - Advance information about the resources deployed is to be communicated and proper hand-over of charge with complete documentation has to be done for the new resources, which should be approved by LIC.
    - All necessary steps/changes have to be effected in security infrastructure as per the requirements of ISO27001, Certifying Authority/ Body etc. or any third party security audit / inspection report.

Note:

- No telephone connection will be provided by LIC to the onsite support persons.
- The on-site L1 and L2 support may also be required to work on Sunday/LIC holidays or beyond office hours on working days, for which an advance notice will be given.

Service-Delivery and Project Management:

The selected vendor will have to post a full-time onsite Service-Delivery Manager (SDM) immediately after the signing of the Contract. The detail of SDM should be conveyed in writing to LIC within 4 weeks of receipt of purchase order. The onsite Service-Delivery Manager will be required to be posted for the entire implementation period and has to sit on site at LIC-CO-IT, Mumbai office. The onsite SDM should have the following minimum profile:

a) Minimum 10 years of IT experience
b) ITIL aware and having knowledge of Service Delivery processes.
c) Minimum 2 years of Program Management experience.
d) 2 years' experience of Network gateway security deployments.
e) Experience of handling/managing teams (Minimum 5 reportees).

The responsibilities of the On-site Service-Delivery Manager as a part of support are as follows (indicative but not exhaustive):

a) Act as a Single Point of Contact (SPOC) for the entire project
b) Responsibility for the entire execution & management of the project after receipt of purchase order. (ii) Overall monitoring of project
c) Coordination for Delivery/Installation of New hardware in stipulated time frame
d) Call flow management, Quality Service Delivery
e) On-site Team management
f) Overall monitoring and management of network gateway security and related services
g) SLA management and reporting
h) Submission of periodical Reviews and reports required by LIC.
i) Crisis management and Emergency response procedures.
j) Preparation and submission of detailed Project documentation to LIC (Purchase Order wise) and progress of initiatives taken by LIC.
k) He should be placed at LIC premises during LIC's office hours. However, the hours may be extended whenever required.

The Vendor shall submit to Executive Director IT, CO, Mumbai the name and contact details, including address, telephone number, mobile number, FAX number/email address of the nominated Service-Delivery Manager.

It is mandatory for the concerned Service-Delivery Manager to have structured meeting with the ED(IT/BPR)/Secretary(IT/BPR)/Dy. Secretary(IT/BPR)/Assistant Secretary (IT/BPR), Network Section of Central Office once a week, preferably on Monday, during the implementation period from the date of receipt of the first Purchase Order by the vendor. Weekly meetings should be held till the project is entirely rolled out.

In short, Onsite Service-Delivery Manager shall carry out and coordinate the various tasks involved in the project like Project scheduling, tracking, monitoring, identifying risks, liasioning with all stake holders (OEM, vendors back-end teams etc.) and reporting to LIC on the overall progress of the project, etc. No charges will be payable by LIC for the onsite Service-Delivery Manager.

6. Project Timelines

The Phase Wise Project Timelines as below:

a. CASB

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
2	Delivery of all the software licenses as quoted in the bill of materials for each solution in-scope.	T + 5 Weeks = D
3	Understanding of the current state, scope, and exclusion of solution implementation.	D+ 4 Weeks = D1
4	Implementation and Integration of in-scope LIC SaaS based applications. Date of implementation of last SaaS LIC application shall be taken as date of installation of all the applications.	D1 + 12 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 4 weeks = D3

6	Transition to manage services	D3 + 4 Weeks = D4 till the end of the contract

b. NAC

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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 + 9 Weeks= D
3	Understanding of the current state, scope, and exclusion of solution implementation.	D+ 2 Weeks = D1
4	Implementation and Integration of in-scope solutions. Date of implementation of last device shall be taken as date of installation of all devices	D1 + 16 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 5 weeks = D3
6	Transition to manage services	D3 + 4 Weeks = D4 till the end of the contract

c. SSL Off loader

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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
3	Understanding of the current state, scope, and exclusion of solution implementation.	D+2 Weeks = D1
4	Implementation and Integration of in-scope solutions. Date of implementation of last device shall be taken as date of installation of all devices	D1 + 12 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 3 weeks = D3
6	Transition to manage services	D3 + 2 Weeks = D4 till the end of the contract

d. WAF

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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 + 8 Weeks= D
3	Understanding of the current state, scope, and exclusion of solution implementation.	D+2 Weeks = D1
4	Implementation and Integration of in-scope solutions. Date	D1 + 14 Weeks = D2

	of implementation of last device shall be taken as date of installation of all devices	
5	The sign-off document of the project, phase, or deliverable	D2 + 3 weeks = D3
6	Transition to manage services	D3 + 3 Weeks = D4 till the end of the contract

e. Mobile Device Management

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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 + 8 Weeks= D
3	Understanding of the current state, scope, and exclusion of solution implementation.	D + 2 Weeks = D1
4	Implementation and Integration of in-scope solutions. Date of implementation of last device shall be taken as date of installation of all devices	D1 + 16 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 5 weeks = D3
6	Transition to manage services	D3 + 4 Weeks = D4 till the end of the contract

f. Server Load Balancer (SLB)

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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
3	Understanding of the current state, scope, and exclusion of solution implementation.	D + 2 Weeks = D1
4	Implementation and Integration of in-scope solutions. Date of implementation of last device shall be taken as date of installation of all devices	D1 + 16 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 5 weeks = D3
6	Transition to manage services	D3 + 4 Weeks = D4 till the end of the contract

g. Virtual Desktop Interface (VDI)

Sr. No.	Activity	Timelines
1	Issuance of Purchase Order to successful bidder	T
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

3	Understanding of the current state, scope, and exclusion of solution implementation.	D+ 4 Weeks= D1
4	Implementation and Integration of in-scope solutions. Date of implementation of last device shall be taken as date of installation of all devices	D1 + 12 Weeks = D2
5	The sign-off document of the project, phase, or deliverable	D2 + 4 weeks = D3
6	Transition to manage services	D3 + 4 Weeks = D4 till the end of the contract