Ref: CO/ERM/IT-CSD **Date: 24.11.2025**

Selection of Service Provider for conducting Compromise Assessment and Incident Response Retainership
CO-ERM-IT-CSD/2025-2026/CA & IRR dated 30th October, 2025

Response to Pre-Bid Queries

This is with reference to the RFP released by the Life Insurance Corporation of India on 30th November, 2025 captioned above. Responses to pre-bid queries to this RFP are given below:

Part-A: Compromise Assessment

Sr. No.	RFP Clause	Bidder Query	LIC Response
1		Will the Bidder be allowed to install custom agents on 35000 machines to perform the compromise assessment activity?	The successful bidder shall be solely responsible for deploying agents on LIC's assets.
2		Is the any list of security device logs i.e. Firewall, WAF, Proxy, IDS/IPS, EDR, DLP, SIEM etc. that needs to be considered for compromise assessment of 35000 machines? If yes please provide security solution list and count of firewalls, devises that are to be considered etc.	This will be informed to the successful bidder.
3		Can the Bidder utilize the existing security monitoring solutions like SIEM, EDR to perform the compromise assessment? Instead of collecting through agents from 35000 machines?	The present solutions available in LIC can be leveraged for CA & IRR by the successful bidder.
4		Time period for the compromise assessment i.e. 1 month or 2 months, for which the logs or data need to be checked.	The Compromise Assessment shall include an analysis of logs from the past six months.
5		Are there any restrictions on the types of tools or agents that can be used (e.g., open-source vs. commercial, agent-based vs. agentless)? Are there any pre-approved or disallowed technologies.	No. The bidder shall provide legally valid software, hardware, and firmware solutions. Detailed information regarding the license count and type of licenses shall be provided to LIC. There shall be no violations of copyrights, trademarks, patents, or any other intellectual property rights, as specified in the RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
6	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest.	Google has acquired Mendicant, a cyber security and incident response services provider. This RFP is a new engagement with no overlap in scope, deliverables, or access, so Google Cloud Platform (GCP) can participate without a conflict of interest. We're requesting a waiver to allow Google (GCP) to bid through the bidder, making both the bidder and OEM eligible. Both Google and bidder have been awarded project with LIC for different services and requesting waiver to participate for this specialized services by Mendicant	Please refer to modification-1.
7	Bidder/OEM should have experience in Compromise Assessment completion in at least five cases in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies/Big companies of turnover more than 500 cores in last 7 years starting from 01.04.2018. Purchase order must be in the name of the bidder.	The CA work carried is confidential due to sensitive information and signing of NDA and integrity pact restricts sharing of the name, references. Request LIC to consider the masked work order for same for services rendered to fulfill this requirement	Please submit the confirmation letter from Customer regarding in progress / successful completion of CA work on customer letter head if purchase order are not provided. In case masking is done, the field required to establish the fulfillment of RFP requirement should be visible.
8	client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India in last 7 years starting from 01.04.2018. (Start and End Date of the Project to be mentioned) in the past (At least two client references are required)	The IRR work carried is confidential and signing of NDA and integrity pact restricts sharing of the name, references. Request LIC to consider the masked work order.	Please submit the confirmation letter from Customer regarding in progress / successful completion of CA and IRR work on customer letter head if purchase order are not provided. In case masking is done, the field required to establish the fulfillment of RFP requirement should be visible.

Sr. No.	RFP Clause	Bidder Query	LIC Response
9	Total information assets to be covered: Around 35,000 information assets covering servers, databases, desktops, appliances like routers, switches, firewall etc.	We understand LIC will facilitate the installation of required agents on 35000+ assets. Kindly provide us the break of the no of desktops (RHEL) Windows servers. We understand its all windows and linux only and no other OS	This will be informed to the successful bidder.
10	Deployment of endpoint detection tools or forensic agents (where applicable) to gather telemetry and logs.	The LIC India host infrastructure teams will need to perform the installation and deployment, as well as de-installation at the end of the engagement as the admins have the previleges for same. Mandiant will provide LIC with the installer for FACT (Forensic Artifact collector Tool). LIC will need to whitelist FACT IP/DNS. The LIC India host infrastructure teams will perform the required changes to support Mandiant tool for the agent communications with the analysis platform.	Please adhere to the terms and conditions of RFP. It is the responsibility of the bidders for installation of required agents on the specified assets.
11	The duration of the engagement would be 1 year for Part-A	We understand the expectation here is to complete the compromise assessment activity for 35000 systems in scope and revalidation of the findings within one year of the stipulated time from project start date	The post-remediation check shall commence within 6 to 9 months after the completion of the Compromise Assessment, or upon LIC's request, within 12 months.
12	To be available on-site within 4 hours	We have globally available resources; kindly clarify LIC's expectations regarding the onsite deployment or presence requirements for this engagement. Also, kindly confirm if bidders' resources can also be considered for this requirement.	Please adhere to the terms and conditions of RFP.
13	General Query	Please confirm whether the Compromise Assessment (CA) and Incident Response Retainership (IRR) activities are expected to run in parallel or will be executed sequentially as separate phases.	CA and IRR are expected as separate as they are separate contracts.
14	No advance payment or interest payment will be made by LIC.	Request LIC to consider the 50% payment after the successful completion of the installation of agents across 35000 system. 25% after the submission of the draft report and remaining 25% after the validation activity is completed	Please adhere to the terms and conditions of RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
15	Further, LIC will make payment towards CA and IRR (over and above 35000 systems), if required, in multiples of 1000 systems based on pro-rata cost of One-time CA cost of 35,000 systems as submitted by the bidder in commercial bid and payment will be released on submission of invoice upon completion of the Compromise Assessment and acceptance of all Project deliverables by LIC.	Please clarify whether LIC can consider making additional payments for systems exceeding the initial 35,000 count . Our services starts with minimum count of 10000 systems hence request LIC to include the same for incremental scope or additional scope to factor	Please refer to RFP and answer to queries.
16	Deployment of tools and technologies in LIC environment & maximum timeline 30 days (T)	Request to extend the deployment timeline to be extended up to 60 working days considering the LIC envoirnment and internal approval processes where dependency will be on the LIC admins to facilitate the same.	Please refer to modification-1.
17	For CA & IRR Onsite availability of the analyst as demanded	The Mandiant services offered is from Global pool of the resources and carry out analysis and activities remotely. The delivery head or engagement director for the IRR services can travel and available in short notice as per RFP. The analyst based out of country will take time to travel as per the need arises.	Please adhere to the terms and conditions of RFP.
18	Total information assets to be covered: Around 35,000 information assets covering servers, databases, desktops, appliances like routers, switches, firewall etc.	We understand LIC will facilitate the installation of required agents on 35000+ assets. Kindly confirm.	Query already answered.

Sr. No.	RFP Clause	Bidder Query	LIC Response
19	Total information assets to be covered: Around 35,000 information assets covering servers, databases, desktops, appliances like routers, switches, firewall etc.	We understand LIC will facilitate the installation of required agents on 35000+ assets. Kindly provide us the break of the no of desktops (RHEL) Windows servers. We understand its all windows and linux only and no other OS	Installation of all tools and technologies etc. will be the responsibility of successful bidder. LIC will provide licenses for Red Hat Enterprise Linux (RHEL) and the MySQL database.
20	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest.	We wish to clarify that our ongoing engagement with LIC is in a completely different functional domain and has no relation to cybersecurity or incident response services. This RFP represents a new, standalone engagement, with no overlap in scope, deliverables, or access, and hence does not constitute a conflict of interest. Hence, requesting you to delete the clause.	Please refer to modification-1.
21	The Bidder or the OEMs who are directly participating should have experience of minimum 7 years in providing the compromise assessment/forensic investigation/Incident Response Retainership Services starting from 01.04.2018.	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
22	Bidder/OEM should have experience in Compromise Assessment completion in at least five cases in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies/Big companies of turnover more than 500 crores in last 7 years starting from 01.04.2018. Purchase order must be in the name of the bidder.	The CA work carried is confidential due to sensitive information and signing of NDA and integrity pact restricts sharing of the name, references . Request LIC to consider the masked work order for same for services rendered to fulfill this requirement	The query has already been answered.

Sr. No.	RFP Clause	Bidder Query	LIC Response
23	client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India in last 7 years starting from 01.04.2018. (Start and End Date of the Project to be mentioned) in the past (At least two client references are required)	The IRR work carried is confidential and signing of NDA and integrity pact restricts sharing of the name, references. Request LIC to consider the masked work order.	Please adhere to the terms and conditions of RFP.
24	The duration of the engagement would be 1 year for Part-A	We understand the expectation here is to complete the compromise assessment activity for 35000 systems in scope and revalidation of the findings within one yr of the stipulated time from project start date	Request to please go through the RFP.
25	To be available on-site within 4 hours	Our technology partner have globally available resources; kindly clarify LIC's expectations regarding the onsite deployment or presence requirements for this engagement. Also, kindly confirm if bidders resources can also be considered for this requirement.	Please adhere to the terms and conditions of RFP.
26	Deployment of tools and technologies in LIC environment & maximum timline 30 days (T)	Request to extend the deployment timeline to be extended upto 60 working days considering the LIC environment and internal approval processes where dependency will be on the LIC admins to facilitate the same.	Please refer to modification-1.
27	For CA & IRR Onsite availability of the analyst as demanded	The Mandiant services offered is from Global pool of the resources and carry out analysis and activities remotely . The delivery head or engagement director for the IRR services can travel and available in short notice as per RFP. The analyst based out of country will take time to travel as per the need arises.	Please adhere to the terms and conditions of RFP.
28	General Query	Please confirm whether the Compromise Assessment (CA) and Incident Response Retainership (IRR) activities are expected to run in parallel or will be executed sequentially as	The activities as given in Part-A and Part-B are separate contracts. The activities will not be performed in parallel manner.

Sr. No.	RFP Clause	Bidder Query	LIC Response
		separate phases.	
29	No advance payment or interest payment will be made by LIC.	Please clarify if LIC can consider a phase-wise payment structure for the Compromise Assessment activity, as it involves a one-time engagement covering approximately 35,000 assets and will be executed in defined phases. This will help ensure smooth project execution and resource allocation.	Please adhere to the terms and conditions of RFP.
30	No advance payment or interest payment will be made by LIC.	Request LIC to consider the 50% payment after the successful completion of the installation of agents across 35000 system. 25% after the submission of the draft report and remaining 25% after the validation activity is completed	Please adhere to the terms and conditions of RFP.
31	Further, LIC will make payment towards CA and IRR (over and above 35000 systems), if required, in multiples of 1000 systems based on pro-rata cost of One-time CA cost of 35,000 systems as submitted by the bidder in commercial bid and payment will be released on submission of invoice upon completion of the Compromise Assessment and acceptance of all Project deliverables by LIC.	Please clarify whether LIC can consider making additional payments for systems exceeding the initial 35,000 count. Our services starts with minimum count of 10000 systems hence request LIC to include the same for incremental scope or additional scope to factor	LIC shall make payment towards Compromise Assessment for systems exceeding 35,000, if required, in multiples of 100 systems. The payment shall be calculated on a pro-rata basis, derived from the cost of 35,000 systems as quoted by the bidder in the commercial bid. Payment will be released upon submission of an invoice after completion of the Compromise Assessment, and upon acceptance of all project deliverables by LIC.

Sr. No.	RFP Clause	Bidder Query	LIC Response
32	Experience in conducting Compromise assessment For each assignment or assessment (2 marks for each assignment executed) in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies in last 10 years starting from 01.04.2015. Documentary proof of order completed / Contract Copy issued in the name of the bidder Please refer Appendix-D2	We understand to meet this requirement; bidders/OEM's credentials will be acceptable. Kindly confirm.	Please adhere to the terms and conditions of RFP.
33	Cost for Post remediation checks	We understand, during the remediation checks, only the devices with suspicious/malicious infections needs to be checked. Kindly confirm if the understanding is correct.	During remediation check, the controls implemented against identified observations needs to be checked. The activity will be performed as per the instructions from LIC.
34	The Bidder or the OEMs who are directly participating, should have experience of minimum 7 years in providing the compromise assessment/forensic investigation/Incident Response Retainership Services starting from 01.04.2015. Experience up to 7 years -> 5 marks Experience more than 7 years but less than equal to 10 years -> 8 marks Experience of more than 10 years -> 10 marks	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
35	Deployment of endpoint detection tools or forensic agents (where applicable) to gather telemetry and logs.	The LIC India host infrastructure teams will need to perform the installation and deployment, as well as de-installation at the end of the engagement as the admins have the previleges for same . Mandiant will provide LIC with the installer for FACT(Forensic Artifact collector Tool). LIC will need to whitelist FACT IP/DNS . The LIC India host infrastructure teams will perform the required changes to support Mandiant tool for the agent communications with the analysis platform.	Please adhere to the terms and conditions of RFP.
36	General Query	Please confirm whether the Compromise Assessment (CA) and Incident Response Retainership (IRR) activities are expected to run in parallel or will be executed sequentially as separate phases.	The query has already been answered.
37		How many users, IT assets (workstations, servers - Windows, Linux, Other)	This will be informed to the successful bidder.
38		How many different type of unique assets? (UAT, PROD, Critical, Non-Critical)	This will be informed to the successful bidder.
39		How many cloud instances you have running across your environments along with the service provider?	This will be informed to the successful bidder.
40		List of cloud platforms and logging tools in use (e.g., AWS CloudTrail, Azure Monitor).	This will be informed to the successful bidder.
41		What will the period of logs (Last 6 Months, 1 year, 2 years) to be reviewed for compromise assessment?	last 6 months log will be reviewed.
42		Please share coverage for tools in SOC like, SIEM, EDR etc.	This will be informed to the successful bidder.
43		Where are logs stored? (e.g., SIEM, cloud blob, local disk, centralized log server)	This will be informed to the successful bidder.
44		What are the log retention period?	This will be informed to the successful bidder.
45		Are archival solutions used for long-term storage? If yes, Please provide details.	This will be informed to the successful bidder.
46		Who manages the SIEM (internal SOC, MSSP, hybrid)?	This will be informed to the successful bidder.

Sr. No.	RFP Clause	Bidder Query	LIC Response
47		What is the current EPS? (Events per second)	This will be informed to the successful bidder.
48		Is your organization adopting or planning to adopt a Zero Trust architecture?	This will be informed to the successful bidder.
49		For Compromise assessment it will be up-to 3-4 resources (time 9:00 AM to 6:00 PM for 5 days in a week), please confirm	The successful bidder is required to strategize to complete the activity in due time as given in the RFP. Office will be kept open from 9.00 AM to 6.00 PM for 5 days as requested.
50		Are micro-segmentation or identity-aware proxies used in the network design?	This will be informed to the successful bidder.
51	Bidder/OEM should have experience in Compromise Assessment completion in at least five cases in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies/Big companies of turnover more than 500 crores in last 7 years starting from 01.04.2018	Request to change to three (3) cases	Please refer to modification-1.
52	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India in last 7 years starting from 01.04.2018	Request to consider copy of agreement / purchase order / email confirmation	Copy of agreement / purchase order/ in progress or successful completion of project will only be considered.
53	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest.	Request to consider only LIC Projects in Cyber Security	Please refer to modification-1.

Sr. No.	RFP Clause	Bidder Query	LIC Response
54	Experience in conducting Compromise assessment For each assignment or assessment (2 marks for each assignment executed) in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies in last 10 years starting from 01.04.2015.	Request to change to 3 marks for each assignment executed	Please adhere to the terms and conditions of RFP.
55	Deployment of Solution: Solutions to be deployed to investigate systems from security point of view including applicable hardware and software infrastructure	What existing SIEM and EDR/XDR solutions are available that can be leveraged for Incident Response and Compromise Assessment by the bidder	The present solutions available in LIC can be leveraged for Incident Response and Compromise Assessment by the successful bidder.
56	Examination of a representative sample of servers, workstations, and laptops	How many endpoints and servers will be included in the representative sample? Will LIC assist with deploying agents on the representative servers?	This will be informed to the successful bidder. Deploying agents on the assets will be the sole responsibility of the successful bidder.
57	Review of email gateway logs and inbox rules for potential business email compromise (BEC) or phishing indicators.	Which email security solution is currently deployed	This will be informed to the successful bidder.
58	Analysis of cloud workloads and storage buckets for misconfigurations or abnormal activity.	Is there already any CSPM suite deployed at LIC, or cloud access and security logs available in the SIEM, or the vendor is expected to provide?	This will be informed to the successful bidder.
59	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of	We wish to clarify that our ongoing engagement with LIC is in a completely different functional domain and has no relation to cybersecurity or incident response services. This RFP represents a new, standalone engagement, with no overlap in scope, deliverables, or access, and hence does not	Please refer to modification-1.

Sr. No.	RFP Clause	Bidder Query	LIC Response
	interest.	constitute a conflict of interest. Hence, requesting you to delete the clause.	
60	Total information assets to be covered: Around 35,000 information assets covering servers, databases, desktops, appliances like routers, switches, firewall etc	We understand LIC will facilitate the installation of required agents on 35000+ assets. Kindly confirm.	Please adhere to the terms and conditions of RFP. It is the responsibility of the bidders for installation of required agents on the specified assets.
61	To be available on-site within 4 hours	We have globally available resources; kindly clarify LIC's expectations regarding the onsite deployment or presence requirements for this engagement. Also, kindly confirm if bidder's resources can also be considered for this requirement.	Please adhere to the terms and conditions of RFP.
62	General Query	Please confirm whether the Compromise Assessment (CA) and Incident Response Retainership (IRR) activities are expected to run in parallel or will be executed sequentially as separate phases.	This will be informed to the successful bidder.
63	No advance payment or interest payment will be made by LIC.	Please clarify if LIC can consider a phase-wise payment structure for the Compromise Assessment activity, as it involves a one-time engagement covering approximately 35,000 assets and will be executed in defined phases. This will help ensure smooth project execution and resource allocation.	Please adhere to the terms and conditions of RFP.
64	Further, LIC will make payment towards CA and IRR (over and above 35000 systems), if required, in multiples of 1000 systems based on pro-rata cost of One-time CA cost of 35,000 systems as submitted by the bidder in commercial bid and payment will be released on submission of invoice upon completion of the Compromise Assessment and acceptance of all	Please clarify whether LIC can consider making additional payments for systems exceeding the initial 35,000 count in smaller increments, such as in multiples of 100 or 10 systems, instead of 1,000, to ensure more accurate billing and flexibility in scope management.	Payment will be made on a pro-rata basis, based on the actual number of hours utilized in multiples of 100 systems to ensure more accurate billing.

Sr. No.	RFP Clause	Bidder Query	LIC Response
	Project deliverables by LIC.		

Part-B : Incident Response Retainership

Sr. No.	RFP Clause	Bidder Query	LIC Response
1		What are the expected SLAs for response times (e.g., maximum time to respond, time to be on-site), and do these differ by incident severity or location?	Please refer to RFP.
2		Who is responsible for remediation activities, and what are the acceptance criteria for a “clean” system prior to migration?	Successful bidder is required to recommend and guide for all observations for remediation activities. The remediation activity will be LIC's responsibility.
3		Can data be processed outside LIC Premises, or must all analysis and storage be performed on-premise within LIC’s environment?	All data need to be processed and analyzed in LIC premises.
4		Are there any restrictions on the types of tools or agents that can be used (e.g., open-source vs. commercial, agent-based vs. agentless)? Are there any pre-approved or disallowed technologies.	NO. The successful bidder will be expected to assume responsibility for all software licenses.

Sr. No.	RFP Clause	Bidder Query	LIC Response
5	For CA & IRR Onsite availability of the analyst as demanded	The Mandiant services offered is from Global pool of the resources and carry out analysis and activities remotely . The delivery head or engagement director for the IRR services can travel and available in short notice as per RFP. The analyst based out of country will take time to travel as per the need arises.	Please adhere to the terms and conditions of RFP.
6	IRR	IRR - Incidence Response & Retainership. Retainership fee is applicable for every year irrespective of services started which depends upon the need for initiating the breach investigation if any incident happen. Incident response services get invoked as per the terms of the RFP once incident is invoked and accordingly the assessment is conducted. So what is the meaning of Assessment for yr 1, Yr 2 and Yr 3. The 800 hours has to be provisioned for first year and may need to repurpose if not utilized for other Mandiant services as per the catalogue of offerings mentioned before the expiry of the annual term	Please adhere to the terms and conditions of RFP.
7		Once the IR begins, no of provisioned hours may extend beyond 800 that require for investigation, please provide info if additional man hour rates need to given or will be done on pro-rata basis for the engagement submitted for 800 hours	If no of hours extend beyond 800 hours, LIC will make payment for extended hours and payments will be done on pro-rata basis. Please refer to Modification-1
8	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest	We wish to clarify that our ongoing engagement with LIC is in a completely different functional domain and has no relation to cybersecurity or incident response services. This RFP represents a new, standalone engagement, with no overlap in scope, deliverables, or access, and hence does not constitute a conflict of interest. Hence, requesting you to delete the clause.	Please refer to Modification-1

Sr. No.	RFP Clause	Bidder Query	LIC Response
9	Man hours cost in 1st Assessment, Man hours cost in 2nd Assessment,Man hours cost in 3rd Assessment,	What does LIC mean by assessment here? Kindly clarify what is to be covered under the assessment 2 and assessment 3. Please clarify.	1st assessment refers to 1st year/assessment, 2nd assessment refers to 2nd year/assessment etc. The activities performed by the bidder will be as per the terms and conditions of RFP. However, the assets as per the RFP may be different.
10	IRR	IRR - Incidence Response & Retainership. Retainership fee is applicable for every year irrespective of services started which depends upon the need for initating the breach investigation if any incident happen. Incident response services get invoked as per the terms of the RFP once incident is invoked and accordingly the assessment is conducted. So what is the meaning of Assessment for yr 1, Yr 2 and Yr 3. The 800 hours has to be provisioned for first year and may need to repurpose if not utlizied for other Mandiant services as per the catalogue of offerings mentioned before the expiry of the annual term	Please adhere to the terms and conditions of RFP.
11	General Query	Once the IR begins, no of provisioned hours may extend beyond 800 that require for investigation, please provide info if additional man hour rates need to given or will be done on pro-rata basis for the engagement submitted for 800 hours	If no of hours extend beyond 800 hours, LIC will make payment for extended hours and payments will be done on pro-rata basis. Please refer to Modification-1
12	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest	We wish to clarify that our ongoing engagement with LIC is in a completely different functional domain and has no relation to cybersecurity or incident response services. This RFP represents a new, standalone engagement, with no overlap in scope, deliverables, or access, and hence does not constitute a conflict of interest. Hence, requesting you to delete the clause.	Please refer to Modification-1

Sr. No.	RFP Clause	Bidder Query	LIC Response
13	Man hours cost in 1st Assessment, Man hours cost in 2nd Assessment,Man hours cost in 3rd Assessment,	What does LIC mean by assessment here? Kindly clarify what is to be covered under the assessment 2 and assessment 3. Please clarify.	Query has already been answered.
14	Experience in conducting Incident Response Retainership For each assignment or assessment (2 marks for each assignment executed) in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies in last 10 years starting from 01.04.2015. Documentary proof of order completed / Contract Copy must be in the name of the bidder. Please refer Appendix-E2	We understand to meet this requirement, bidders/OEM's credentials will be acceptable. Kindly confirm.	Please adhere to the terms and conditions of RFP.
15	Man-hour cost for Incident Response Retainership Services for 720 man hours	We seek clarification to understand how will LIC compensate if the IRR services go beyond the 720 hours. We request LIC to kindly include separate line item in mentioned BOQ of Part B to ensure the additional man hour efforts are compensated.	Query has already been answered.
16	Man hours cost in 1st Assessment, Man hours cost in 2nd Assessment,Man hours cost in 3rd Assessment,	Kindly clarify the frequency of this assessment which needs to be carried out. We understand LIC expects to conduct the assessment annually for 35000 assets. i.e. assessment 1 will be for first year, Assessment 2 for second year and assessment 3 for third year. Kindly confirm.	The same will be informed.

Sr. No.	RFP Clause	Bidder Query	LIC Response
17	The Bidder or the OEMs who are directly participating, should have experience of minimum 7 years in providing the compromise assessment/forensic investigation/Incident Response Retainership Services. Experience up to 7 years -> 5 marks Experience more than 7 years but less than equal to 10 years -> 8 marks Experience of more than 10 years -> 10 marks	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
18	The OEM or the bidder who are directly participating should have experience of minimum 7 years in providing the Incident Response Retainership Services starting from 01.04.2018.	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
19	Provide incident response engagements have Bidder had in the past three (3) years involving APT group intrusions. Provide examples of the nature of the intrusion and major activities that Bidder performed, or consulted with the customer organization to perform, in the past three (3) to remediate the intrusion.	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
20	Provide redacted incident response engagements have Bidder had in the past three (3) years involving ransomware attacks. Provide examples of the nature of the intrusion and major activities that	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
	Bidder has performed.		
21	Provide the experience Bidder"s analysts have with malware analysis along with the tools used for incident response.	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
22	Bidder should have an experience presenting information about incidents to a Board of Director level body. Provide details of Bidder"s staff have this type of experience. .	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
23	The resources /consultants engaged in the activity must have at least 5 years hands on experience in identifying compromises and responding to security breaches.	We request to consider OEM's credentials as acceptable in case bidder participates with OEM.	Please adhere to the terms and conditions of RFP.
24	The bidder must able to provide Signatures, YARA rules, detection rules, block rules for the solution deployed in LIC environment such AV, SIEM, EDR, IDS/IPS, WAF, Load balancer, NBAD, Active Directory, etc. in order to detect the presence of IOC or revert the back the changes made by the attacker.	We understand , LIC & its existing SOC team will be making the required changes in configuration of their existing security solutions. Kindly confirm the understanding.	LIC & its existing SOC team will confirue or implement the required changes based on the recommendations or advisories.

Sr. No.	RFP Clause	Bidder Query	LIC Response
25	The selected vendor will help LIC to prepare and regularly update IRR Playbooks for LIC.	We understand that the responsibility of preparing and maintaining the IRR Playbooks rests with LIC. The bidder's role will be limited to notifying LIC about the need for preparing or updating the playbooks based on changes in the environment or threat landscape. Kindly confirm our understanding.	Review of current IRR playbook will be required along with recommendation to update the playbook based on changes in the environment or threat landscape.
26	The Service provider should start the Incident Response within 4 Hours of reporting of alert from LIC. Upon confirmed breach, the IR analyst should immediately start working on preliminary information submitted by LIC. The IR analyst should be at onsite location of breach, if required, as per timelines mentioned in this RFP.	Kindly elaborate the expectations here. WE understand, online support is sufficient to meet the functional requirement of the project & same will be acceptable to LIC.	Please adhere to the terms and conditions of RFP.
27	The vendor should assist LIC in identifying and mitigating all vulnerabilities that were exploited by the Threat Actor.	We understand that the vendor's role will be limited to providing advisory support and recommendations for identifying and mitigating the vulnerabilities exploited by the threat actor, while the actual remediation will be carried out by LIC's internal team. Kindly confirm our understanding.	Yes
28	The vendor should restore the attacked system/ operations to normal state and should ensure that the systems are functioning normally and remediate vulnerabilities to prevent similar incidents.	We understand that the vendor's role will be limited to providing incident response guidance and recommendations for restoration and remediation, while the actual system restoration and implementation of fixes will be performed by LIC's internal IT team. Kindly confirm our understanding.	Yes.

Sr. No.	RFP Clause	Bidder Query	LIC Response
29	Phase 6 Recovery/Monitoring: In this phase, the incident response team works to restore normal business operations and ensure that all systems are functioning properly. This shall also involve conducting user awareness training, updating policies and procedures, and reviewing incident response plans. The bidder should perform continuous monitoring of the network/in for the agreed period of time based on the severity of incident in order to make sure that there is no remanence of the threat actor left in the network.	We understand that the bidder's role will be limited to providing recommendations, advisory support, and periodic review reports during the recovery and monitoring phase, while the continuous monitoring of the network and infrastructure will be performed by LIC's in-house team or their designated SOC. Kindly confirm our understanding.	Yes.
30		What response time expectations do you have (e.g., SLA for critical incidents)?	Please refer to Section-F.
31		Resources will be deployed on-site based on the activity for incident analysis, in an hybrid approach, please confirm	Yes.
32		How many tabletop exercises do you want to conduct in a quarter ?	One IR assessment should be considered as one activity. Hence applicable IR simulations are required to be conducted as per terms and conditions of RFP. It is not a quarterly activity.
33		How many IR simulations do you want to conduct in a quarter? (Ransomware, Data exfiltration etc.)	One IR assessment should be considered as one activity. Hence applicable IR simulations are required to be conducted as per terms and conditions of RFP. It is not a quarterly activity.
34		Do you have an existing Incident Response Plan (IRP)? If yes, when was it last reviewed or tested?	This will be informed to the successful bidder. The IRP document will required to be created. Please refer to Modification-1.
35		How many IR play book do you currently have?	This will be informed to the successful bidder.

Sr. No.	RFP Clause	Bidder Query	LIC Response
36	Bidder/OEM should have experience in Compromise Assessment completion in at least five cases in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies/Big companies of turnover more than 500 crores in last 7 years starting from 01.04.2018	Request to change to three (3) cases	Please refer to Modification-1.
37	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India in last 7 years starting from 01.04.2018.	Request to consider copy of agreement / purchase order / email confirmation	Please adhere to the terms and conditions of RFP.
38	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest.	Request to consider only LIC Projects in Cyber Security	Please refer to Modification-1
39	Experience in conducting Incident Response Retainership For each assignment or assessment (2 marks for each assignment executed) in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies in last 10 years starting from 01.04.2015.	Request to change to 3 marks for each assignment executed	Please adhere to the terms and conditions of RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
40	Experience in conducting Incident Response Retainership For each assignment or assessment (2 marks for each assignment executed) in BFSI sector having Min. 500 branches /Govt. Sector in India/regulatory bodies in last 10 years starting from 01.04.2015.	Request to confirm that the assignments would cover any of the following - (Supporting Document: Bidder should provide copies of the Letter of acceptance (LoA) / work order / contract / completion certificate/ incidence response covered under security operations centre / confirmation email for relevant experience.	Please adhere to the terms and conditions of RFP.
41	Bidder is required to factor/provide Hardware/Software Infrastructure along with applicable licenses under this project and the same will be deployed on premise for Compromise assessment.	Will the same be applicable for Incident Response Retainership also?	Following will be provided by LIC: Operating system RHEL and database license Mysql. Software licenses other than RHEL and Mysql will be procured, installed by the successful bidder as per the terms and conditions of RFP which shall be informed to LIC. Please refer to Modification-1.
42	Locations covered under this scope: i. All assets connected to internet and interdependent assets/applications present in Central office or other locations and ii. Critical assets in LIC"s 8 data center	What is the name of centralized location and locations of 8 data centres in the LIC which are to be covered for IRRA?	Centralized location is Mumbai. 5 data centre are in different locations. 3 Data centres are there in Mumbai.
43	Locations covered under this scope: i. All assets connected to internet and interdependent assets/applications present in Central office or other locations and ii. Critical assets in LIC"s 8 data center	Please suggest which overseas locations are expected to be covered and would initial remote support be allowed?	All locations are in India.
44	Total information assets to be covered: Around 35,000 information assets covering servers, databases, desktops, appliances like routers, switches, firewall etc.	How many applications and servers are expected to be covered under IRRA?	This will be informed to the successful bidder.

Sr. No.	RFP Clause	Bidder Query	LIC Response
45	Point No. 2 Phase 1 Incident Response Readiness Assessment (IRRA) Which includes cost of deployment of sensors, agents, Hardware, software, tools etc. (Maximum of 80 Man hours)	If the hours for IRRA exceed 80 hours how will they be covered/adjusted?	Payment will be made on a pro-rata basis, based on the actual number of hours utilized to ensure more accurate billing. Please refer to modification-1.
46	Point 6: The Bidder or the OEMs who are directly participating should have experience of minimum 7 years in providing the compromise assessment/forensic investigation/Incident Response Retainership Services starting from 01.04.2018	Will Engagement Letter Contract copy be eligible where Work Order has not been issued in compromise assessment/ forensic investigation/ Incident Response Retainership Services?	Yes. The document must be in line with our requirement for eligibility criteria and technical bid requirements.
47	SKILL and Experience of resources deployed for Incident Response: The incident responders should be holding at least any two of the following professional certifications	Can the digital forensic certifications like EnCE or ACE also be counted in professional certifications for Incident Response. Will other Digital Forensic certifications be acceptable?	Please adhere to the terms and conditions of RFP.
48	Phase 4 - Analysis: This phase will involve analyzing the incident to determine the scope, cause, and extent of the damage. The IR team may further gather and examine evidence, interview witnesses, and use forensic tools to identify the attacker and their methods	Is there an SLA or minimum criteria set for completing RCA of an incident within defined man days? Regarding Forensic Tools, will the bidder utilize its own tools, hardware and software along with licensing costs or will LIC also provide access to its own tools for forensic examination and analysis? Can the Incident Response analysis be done in bidders premises also or will it be done in LIC location only? Will the Hard Disk drives be provided by LIC for creation and management of Forensic Evidence or will it be billed seperately by	For SLA, please refer to the terms and conditions of RFP. Regarding forensic tool, it will be the bidder's responsibility for software to be procured. Please refer to Modification-1.

Sr. No.	RFP Clause	Bidder Query	LIC Response
		bidder basis each incident?	
49	Point D (i) The successful vendor should conduct two in-person workshop/ hands-on trainings for LIC"s official, during the contract period. The content of the training/workshop will be such that it should facilitate LIC"s team members in responding to Cyber Security incident. Three days of Incident Response training and certification for LIC"s Security team aligned with IRR Activities should be provided by the vendor. The successful vendor shall arrange to provide Hands-on simulation based training on well-known Cyber Security Incidents.	Please specify the frequency of trainings and Please specify the locations where the team is required to conduct the training sessions.	Two training sessions are to be provided for LIC officials: the first shall be conducted after the completion of the first assessment, and the second following the completion of the second assessment. The location for both trainings will be Mumbai.
50	Point vii. The vendor will setup the dedicated IT infrastructure for LIC within India, either physical or in cloud instance (cloud region should be located within India or specific the region of the Incident occurrence), which will be utilized and accessed remotely by IRR analysts, during incident response for log analysis and correlation. No logs or metadata should be transferred outside of India.	Will the cost of setting up dedicated IT infrastructure for Incident Response Readiness be born by bidder or LIC and who will manage the procurement for the same: bidder or LIC?	LIC will provide operating system RHEL and database license Mysql. Software licenses other than RHEL and Mysql will be procured, installed by the successful bidder as per the terms and conditions of RFP which shall be informed to LIC.. The bidder shall provide legally valid software, hardware, and firmware solutions. Detailed information regarding the license count and type of licenses shall be provided to LIC. There shall be no violations of copyrights, trademarks, patents, or any other intellectual property rights, as specified in the RFP.

Sr. No.	RFP Clause	Bidder Query	LIC Response
51	Point x. The successful vendor should establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis, and	Will the hard disk drives for Incident Management provided by LIC or bidder. Will the licensing cost for forensic software billed incident to incident basis?	Please refer to Modification-1.
52	Point No. 3: IRR services (annual charges)	Will the hard disk drives for Incident Management provided by LIC or bidder. Will the licensing cost for forensic software billed incident to incident basis?	Please refer to Modification-1.
53	Phase 2: Incident Identification – The remaining man hours will be utilized in onwards phases, on actual utilization and deployment of IRR services.	Is there any criteria for capping of number of resources required for responding to Incident after Identification	NO.
54	Point xv. This phase will involve identifying a potential incident by collecting and analyzing data from various sources, such as intrusion detection systems, log files, applications, devices and network traffic.	Who will be responsible for identifying Incident for analysis, SOC team, SIEM team or Information Security Team or will there be a dedicated SPOC from LIC?	SPOC details will be provided to successful bidder.
55	Point xvi. 24 * 7* 365 days dedicated India and domestic support facility for incident response shall made available by the vendor. The vendor IRR staff should be well trained to effectively handle queries raised by LIC, whenever a phone call/ email /alert received from LIC"s dedicated Officials for probable incident.	Is there a minimum SLA criteria defined for making the resource available in India which requires travel to other cities in terms of time? Will the IR Analyst report to any particular location after incident is confirmed, if yes kindly specify. Will the cost of Hard Disk Drives and OPEs (Travel, Stay and Meal) of IR analyst be billed and included Incident to incident basis or be billed separately	Please refer to Section-F for availability of resources. The analyst will require to report to the location where incident happens. However, the analyst is required to report mainly to Mumbai. The cost of hard disk drives shall be reimbursed by LIC, Please refer to Modification-1. Travel related details will be provided in Modification-1.

Sr. No.	RFP Clause	Bidder Query	LIC Response
56	Point xxviii. Root cause analysis of the incident for corrective actions to be submitted to LIC for improvements in robustness and resilience in Cyber Security posture of LIC"s IT infrastructure	Is there a minimum number of days or a timeline defined to come up with RCA and final report Will the RCA report be shared with external agencies like regulatory authorities and Law Enforcement?	Critical observations shall be informed immediately within 1 day from the date identification. Yes, the report will be shared to external agencies.
57	Point xxx. Upon submission of final report, the successful bidder shall not retain any data, and all hard drives consumed will be completely wiped out and reused by the successful bidder in future.	Will the hard disk drives being used and then reused be billed separately for each incident or just once?	The hard disks used in the first assessment will be handed over to LIC for use in subsequent assessments. Billing for these hard disks will be done as part of the first assessment. If new hard disks are required for future assessments, the cost will be billed to LIC. Bidders are requested to share the total cost of Hard drives in commercial bid document. The no. of hard drives, storage capacity, configuration etc. shall be given in the technical bid document. For details, please refer to modification-1.
58	The selected vendor shall provide up to a maximum of 800 man-hours of Incident Response Retainership (IRR) services.	After 800 hours the criteria states that the payment for additional hours after 800 hours will be made on pro-rata basis applicable for that year based on man hours quoted in the commercial bid document, kindly clarify	Payment will be calculated on a pro-rata basis, determined by the actual number of systems covered, rounded to the nearest multiple of 100. This ensures more accurate billing. As a result, the cost may increase if the number of systems exceeds 35,000, or decrease if it falls below 35,000. Please refer to Modification-1.
59	Point Number 2: Phase 1 Incident Response Readiness Assessment (IRRA) Which includes cost of deployment of sensors, agents, Hardware, software, tools etc. (Maximum of 80 Man hours)	What is the location where the IRRA will be performed?	Mumbai

Sr. No.	RFP Clause	Bidder Query	LIC Response
60	Point a. The bidder needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the bidder would need to provide the same without any charge. Bidder should make no changes to the quantity.	We assume the recurring costs will include forensic hardware, software license renewal and other IT support peripherals? Kindly Confirm.	Yes.
61	Point 5 Appendix E5: Compromise (IOC) and Threat Intelligence. References to 25 MITRE Attack.	Request to remove this clause or make as desirable	Desirable clause.
62	Phase 1 Incident Response Readiness Assessment (IRRA) Which includes cost of deployment of sensors, agents, Hardware, software, tools etc. (Maximum of 80 Man hours)	Will the sensors, agents, Hardware, software, tools etc. of LIC also can be used and included for performing IRRA?	Yes.
63	Vendors and OEMs currently engaged in LIC projects awarded through previous RFPs shall not be eligible to participate in this RFP, due to a potential conflict of interest	We wish to clarify that our ongoing engagement with LIC is in a completely different functional domain and has no relation to cyber security or incident response services. This RFP represents a new, standalone engagement, with no overlap in scope, deliverables, or access, and hence does not constitute a conflict of interest. Hence, requesting you to delete the clause.	Please refer to Modification-1
64	Man hours cost in 1st Assessment, Man hours cost in 2nd Assessment,Man hours cost in 3rd Assessment,	What does LIC mean by assessment here? Kindly clarify what is to be covered under the assessment 2 and assessment 3. Please clarify.	The query has already been answered.

Tools and Technologies related queries

S.No	Domain	Tool Category	Tool Name(s)	Vendor	Cloud/On-Prem/Hybrid	Logs Sent to SIEM (Y/N)	Notes (if any)	Response from LIC
1	Data Layer							This will be informed to the successful bidder.
2	End-Point Layer							
3	Network Layer							
4	Perimeter Layer							
5	Application Layer							
6	Identity & Access							
7	Threat Intelligence & analysis							
8	Mobile Device Management							
9	Cloud Security							
10	Vulnerability Management							

Executive Director (ERM) & CRO