Selection of Service Provider for
Incident Response Retainership
Annexure-D

CO-ERM-IT-CSD/2025-2026/IRR dated 9th January, 2026

Enter Bidder's Name

Instructions

1 . Bidder has to compulsorily comply for all items.
2 . Excel Cells where Bidder has to input values, are unlocked.
3 . Print outs of all sheets are required to be duly signed, stamped and submitted.
4 . Reference may be made to the RFP for details.
5 . The bidder can provide the quotes only in coloured cells.

Bidder's name	0

Selection of Service Provider for
Incident Response Retainership
Annexure-D

CO-ERM-IT-CSD/2025-2026/IRR dated 9th January, 2026

Annexure – D: Technical Bid Document (Appendix D1 - Scope of Work and deliverables - Incident Response Retainership)

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
A.	**Mandatory requirements for Service Provider/OEM**				
i.	Service provider must have at least 7 years of experience in incident response and forensic investigations related to Cyber Security incidents in Information Technology Infrastructure, across India and globally.				
ii.	Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorized by specific APT groups, especially Threat event occurrences in Asia-India Region and in financial sector around the globe.				
iii.	Service provider must use combination of their own tools, scripts, inbuilt tools in available in Operating system wherever applicable to perform the incident investigation in order to collect telemetry data across Perimeter, Network & Endpoint.				
iv.	The tools used by Service provider must include custom built tools as well as commercially available products such as Network sensors and log collector.				
v.	The tools used by Service provider must support telemetry data collections from IT Networks / Systems / Endpoints.				
vi.	If required, the service provider must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.				
vii.	As part of the engagement, the service provider shall support in all subsequent phases of incident management lifecycle – triage / analysis, containment, eradication and recovery, and post-incident review.				
viii.	The service provider shall be equipped with tools and processes to ensure chain of custody is maintained throughout the engagement, secure handling (during incident response) and secure disposal of information (upon completion off incident response).				
ix.	Extensive library of Indicators of Compromise (IOC) and Threat Intelligence should be utilized during assessment to analyze network traffic, servers, PCs, network devices, and critical log data during assessment.				
x.	Service provider must have in-house capabilities or past experience to engage with law enforcement agencies and CERT-In to aid in investigations. Public reference on case studies of your engagement with law enforcement agencies shall be provided.				
xi.	The Service provider must have responded to more than 50 cyber security incidents in last 10 years India, out of which at least 5 belongs to incident response in BFSI sector.				
xii.	The Service provider must have cumulative experience of 5000 hours in last five year in cyber security investigations.				
xiii.	The Service provider must have more than 25 MITRE Attack references.				
xiv.	The Service provider must be able to provide profiles of at least 5 Advanced Persistent Threat (APT) / Threat Actor groups with comprehensive insights built based on tracking-of and responding to threats/breaches originating from these APT groups.				
xv.	The Service provider must have dedicated team of more than 50 Security Researchers, Analysts, and Incident Responders.				
xvi.	At least five (5) relevant client references for incident response shall be provided, for each reference include (client name may be redacted to comply with NDA); • Nature of the engagement, dates of the engagement, • Name (or description) of the client firm, and a summary of the activities Bidder performed. • If necessary, references can be interviewed via blind conference calls to protect Bidder's previous clients' confidentiality.				
xvii.	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.				
xviii.	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 Bidder has performed.				
xix.	Provide the experience Bidder's analysts have with malware analysis along with the tools used for incident response.				
xx.	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. .				
xxi.	Provide at least three (3) sample (redacted) final report for an incident response engagement.				
xxii.	Provide five (5) sample resumes that represent a typical team. Names of the individuals are not necessary.				
xxiii.	LIC will be responsible to provide all the hardware required for solution implementation, i.e. server/Virtual Machines and will provide RHEL OS and Mysql, if required as part of the solution. All other software (database, application etc.) required for this project should be provided by bidder, included in BoQ and prices quoted for in the Commercial Bid Document.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
xxiv.	The bidder must supply a thorough inventory of the hardware components required for the planned implementation. This bill of Quantity (BoQ) as per Annexure K should be itemized separately for all the environments, including DC, UAT and Disaster Recovery (DR). The BoQ should include, but is not limited to, the following details: In Scope solutions Components • Site/Environment • Type (VM/Physical) • OS name other than RHEL • Mysql as database license • Database details, if other than Mysql • CPU/vCPU • VLAN requirement (VLAN or Internet) • RAM • Hard Disk Size • Software pre-requisites (.NET framework, IIS, IE, any other OS services, etc.) • If any missing requirements are discovered during installation, and the bidder will be obliged to provide them free of cost.				
B.	**SKILL and Experience of resources deployed for Incident Response**				
i.	The resources /consultants engaged in the activity must have at least 5 years hands on experience in identifying compromises and responding to security breaches.				
ii.	The incident responders should be holding at least any two of the following professional certifications: • GIAC Cyber Threat Intelligence (GCTI), or • GIAC Certified Forensic Analyst (GCFA), or • GIAC Certified Incident Handler Certification (GCIH) or • EC-Council Certified Incident Handler v2 (E|CIH), or • Certified Information Systems Security Professional (CISSP) or • GIAC Cloud Forensics Responder (GCFR) or • GIAC Network Forensic Analyst (GNFA) or • GIAC Reverse Engineering Malware Certification (GREM) or • Computer Hacking Forensic Investigator (CHFI) or • Offensive Security Certified Professional (OSCP)				
iii.	The consultants engaged in the activity must have at least 3 years of hands on experience in threat hunting / malware/ IOC analysis.				
iv.	The consultants engaged in this activity must have experience of dealing with Compromise assessment and Incident response projects of multinational financial institutions.				
v.	The consultants engaged in this activity must have at least 3 years hands on experience with SOC, either in advisory or operational capacity.				
vi.	The consultant shall engage resources for implementation of various job activities required to complete this assessment by giving a detailed item wise plan of action.				
C.	**Methodologies for handling of Cyber Incident and Response**				
i.	The Bidder must be able to Conduct host-based sweeping activities.				
ii.	The Bidder must be able to search for malware and tools linked to specific attack groups that are collectively known as Advanced Persistent Threat (APT) groups.				
iii.	The Bidder must be able to utilize a mix of automated and manual techniques to identify indicators of compromise.				
iv.	The Bidder must be able to search for various artifacts not limited to: staging paths, persistence mechanisms, lateral movement mechanisms, registry keys, etc.				
v.	The Bidder must have to capability to sweep the Endpoint with IOC's related to Custom Malware looking for Persistence Mechanism and Lateral Movement techniques.				
vi.	The Bidder must be able to scan windows end points, Linux end points, servers and virtual environments as a part of the compromise assessment to identify evidence of compromise.				
vii.	The Bidder must have an ability to scan different flavors of Windows, Linux, Unix etc. environments for evidence of compromise.				
viii.	The Bidder must be able to also search for malware and tools associated with non-APT groups.				
ix.	The Bidder must inspect IT systems for IOCs Identifying file names and hashes of known malware and utilities.				
x.	The Bidder must inspect IT systems for IOCs Analyzing file import tables of each executable file for specific IOCs.				
xi.	The Bidder must inspect IT systems for IOCs Reviewing all running processes and network connections for references to known “hostile” domains.				
xii.	The Bidder must inspect IT systems for IOCs Inspecting registry keys and values associated with known malware, and for persistence mechanisms that could lead to the detection of unknown malware.				
xiii.	The Bidder must inspect IT systems for IOCs Identifying specific global mutexes used by processes.				
xiv.	The Bidder must inspect IT systems for IOCs Detecting rootkits, hidden files, hidden processes etc.				
xv.	The Bidder must be able to analyses Web Shells for evidence collection.				
xvi.	The Bidder must be able to analyze event logs generated from different IT systems for evidence collection.				
xvii.	The Bidder must be able to automate collection and analysis of evidence and minimize manual activities.				
xviii.	The Bidder must be able to analyse a majority of assets (at least 85% or higher) and not limit to dipstick analysis on a limited set of assets.				
xix.	The Bidder must be able to Conduct network monitoring activities.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
xx.	The Bidder must have the capability to sweep the Network with IOC's related to Custom Malware looking for Lateral Movement techniques.				
xxi.	The Bidder must be able to monitor the Network traffic for Backdoor command and control protocols.				
xxii.	The Bidder must be able to monitor the Network traffic for Communication to IP addresses that are associated with targeted attacker activity.				
xxiii.	The Bidder must be able to monitor the Network traffic for Resolution of domain names that associates with targeted attacker activity.				
xxiv.	The Bidder must be able to monitor the Network traffic for Certificates that are used by attackers to encrypt malicious traffic.				
xxv.	The Bidder must be able to Conduct log data analysis activities.				
xxvi.	If required, the Bidder must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.				
xxvii.	If required the Bidder should be able to assist for an incident response, from the initial detection to the final resolution of the incident.				
xxviii.	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.				
xxix.	Bidder must be able to perform non-intrusive IRR activities such as log collection, scanning activity, IOC scans using inbuilt tools in cases if agent installation or vendor proposed tool installation is not possible.				
xxx.	The bidder shall identify and document all potential entry points through which cyber attackers may gain access to the network.				
xxxi.	The bidder shall review and update the existing "Cyber Crisis Management Plan" to ensure it includes clearly defined roles and responsibilities.				
D.	**WORKSHOPS**				
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.				
E.	**ANALYSIS AND REPORTING OF INCIDENTS**				
i.	The various Incident Response handling process, analysis, reporting should follow the standard frameworks such as NIST, Lockheed Martin cyber kill chain process, MITRE ATT&CK, diamond model etc.				
ii.	The Security Vendor must be able to provide comprehensive detail of compromise(s) and attack flow(s) if LIC is found compromised.				
iii.	The Security Vendor must be able to Provide Executive reports for Senior Management and non-technical stakeholders with the details of the scanning results and evidence.				
iv.	The Security Vendor must be able to analyse and provide context and intel related to any evidence(s) of compromise found instead of purely enumerating list of the same.				
v.	At the end of the any particular IRR activity, Bidder should provide written confirmation that the infrastructure is free of threat/infection, or the presence of threat actor is seen after agreed monitoring time from both parties.				
vi.	Draft report of the incidents to be vetted by LIC. Reports should not be shared to unauthorized entities without written consent from LIC.				
vii.	Draft detailed report for law enforcement agencies, regulators, communication with internal and external stakeholders.				
F.	**DELIVERY OF IRR SERVICES AND SCOPE**				
i.	**Phase 1: Incident Response Readiness Assessment (IRRA).** This phase will Improve LIC's Incident Response Plan and Procedures. In this phase vendor will help LIC to establish an incident response capabilities so that LIC is ready to respond to it. Under this preparation phase, this involves preparing for potential cyber incidents by establishing incident response plans, identifying the procedural and technical gaps in existing IT Setup w.r.t. incident response readiness, creating an incident response team representative from LIC and IRR vendor personals, defining roles and responsibilities, and implementing monitoring and detection systems. Workshops/assessment to be conducted with various stakeholders in LIC in order to understand LIC environment to enable to Bidders Incident response team to respond, mitigate, recover from attacks as soon as possible. This phase is to review LICs existing Incident response plans, technologies deployed, log sources in place to detect/analyses to be checked and reediness in order to respond to attacks/breaches within stipulated timelines.				
ii.	The vendor should perform the gap assessment on existing SOP of Cyber Security incident handling/ Cyber crisis management plan and various other procedure documents.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
iii.	The IRRA should not be only limited to meetings/workshops/trainings, but Infrastructure manipulation capabilities also to be assessed based on various real time use cases, but not limited to; 1. Centralized deployment/execution of IOC scanners or other tools designed to obtain digital evidence. 2. Credentials management (e.g. password change policies) 3. System backup architecture and backup recovery. 4. Logging security event sources 5. Log sources / security controls check. 6. Assessment of readiness to respond, mitigate, recover from various attack scenarios, but not limited to; i. Espionage by threat actors (including state-sponsored groups) , ii. Watering hole attacks iii. Trusted relationship attacks , iv. Supply chain attacks , v. ATM jackpotting , vi. Ransomware attacks vii. Unauthorized access to servers , viii. Unauthorized access to databases ix. Unauthorized access to web applications or security bypass attacks , x. Unauthorized access to network equipment xi. Insider attacks (leaks) , xii. Insider attacks (disruption, sabotage) , xiii. Insider attacks (unauthorized access) xiv. Insider attacks (unauthorized crypto-currency mining) , xv. Infection using botnets. xvi. Phishing campaigns (links) , xvii. Phishing campaigns (attachments) , xviii. Crypto-currency mining malware attacks xix. Cyber-physical attacks 7. The log sources / security controls should include, but not limited to i. Active directory logs , ii. Network traffic logs , iii. Event logs from endpoints and servers (at the OS, database and application level) , iv. EDR , v. SIEM , vi. VPN connection logs , vii. Web access logs , viii. Antivirus software logs ix. Authentication logs, x. Logs of user authorization and activities on business systems xi. Audit logs of user actions on virtual machine servers Checking sources and performance of SIEM systems xii. Email etc.				
iv.	The vendor will help LIC to prepare incident response team's specific technical methods, strategies, checklists, and forms based on gap assessment.				
v.	The vendor will provide recommendations on how to improve incident response readiness.				
vi.	The vendor will provide recommendations on how to reconfigure or upgrade existing security event monitoring.				
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. The cloud instance should be preserved at least for 3 years of end of contract or based on agreed retention period as per LIC written confirmation.				
viii.	MITRE ATT&CK coverage for the most valuable tactics, techniques, and sub-techniques.				
ix.	During Incident response readiness review exercise the vendor should clearly define below modalities in detail. • Incident Response Retainership team structure and responsibilities • Communication between different teams (Stakeholders from LIC) will took place in case of Cyber Incident • Procedure of sharing evidence / access to the required logs. • The selected vendor will help LIC to prepare and regularly update IRR Playbooks for LIC.				
x.	Establishing required Infrastructure to handle Cyber Incident/ sharing evidence: • The successful vendor should establish a process, and deploy/install necessary hardware, software, sensors, scripts, agents for collection of evidence for incident analysis, and • Assist in clearing/signoff of Comprehensive security review (CSR) of such tools, devices, and technologies before completion of Phase 1 (IRRA)				
xi.	Recommendations on how to reconfigure or upgrade existing security event monitoring systems, backup solutions, security devices, etc.				
xii.	Incident Response Readiness Assessment Report.				
xiii.	Incident Response Readiness Assessment Guide.				
xiv.	**Phase 2: Incident Identification –** The remaining man hours will be utilized in onwards phases, on actual utilization and deployment of IRR services.				
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.				
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.				
xvii.	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.				
xviii.	**Phase 3 – Containment:** In this phase, the IR (incident response) team will work to contain the incident to prevent the further damage to IT assets. This may involve, and not limited to, isolating affected systems, disconnecting them from the network, or shutting them down.				
xix.	The vendor should help LIC to contain the Cyber Security Incident and to eliminate components (Malware, Threat actor) of the Cyber Security Incident.				
xx.	The vendor should assist LIC in identifying and mitigating all vulnerabilities that were exploited by the Threat Actor.				
xxi.	**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.				
xxii.	Log retention and the logs collected/processed should be available for export in supported formats and not associated without any proprietary formats for audit/compliance purposes.				
xxiii.	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.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
xxiv.	The vendor should be able to perform investigation on different technologies, assets inclusive of all technologies, applications, devices residing in LIC's IT-Ecosystem and the various resources required during the investigation should be scalable.				
xxv.	**Phase 5 Eradication:** This phase involves removing the threat and restoring affected systems to their original state. For example, this may involve deleting malware, applying software patches, recommendation of closing vulnerability, exploit used by the threat actor to gain access to the network or restoring from backups. It should be made sure that eradication of threat is to be carried out without disruption to the business.				
xxvi.	**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.				
xxvii.	**Phase 7: Reporting & Lesson learned: The successful vendor should provide**				
xxviii.	Threat Briefing with Executive Board Members. Assist in reporting and notification to Regulatory and statutory authorities, Law Enforcement Agencies, communication to external and internal customers, LIC's Corporate communication handling Public Relations &. Social Media Department, Human Resource Department, News publication etc. 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.				
xxix.	In the final phase, i.e. lesson learned, for improvement in Incident Response capabilities of LIC. The incident response team should conduct a post-incident review to identify what worked well and what could be improved for future incidents. The IR team must give inputs to update LIC's incident response plan and suggest action plan for implementing necessary changes.				
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.				

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted.

Signature of Bidder/Bidder's Representative

Date, Stamp and Seal of the Company

Bidder's name	0

Selection of Service Provider for
Incident Response Retainership
Annexure-D

CO-ERM-IT-CSD/2025-2026/IRR dated 9th January, 2026

Annexure – D: Technical Bid Document (Appendix D2 - Scope of Work and deliverables - Forensic Investigation on Demand)

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
A.	**Information Gathering**				
i.	Understand the chronology of events leading to the incident as well as incident reports (if available) based on assessment done by different service providers/OEM's/Vendors.				
ii.	Obtain an understanding of underlying IT infrastructure (including but not limited to) Server's configuration, existing EDR/security solutions, firewall details, network security configurations, antivirus details and the SIEM applications integration, if any•				
iii.	Assess the nature & quantum of information available for analysis.				
iv.	Identify the data points to be collected and analyzed.				
v.	Understand the nature & quantum of logs/information available for analysis.				
vi.	Understand the roles of various internal and/or external stakeholders involved in the incident.				
B.	**Forensic investigation**				
i.	Perform forensic imaging and acquisition of the identified devices, data, system artefacts and / or relevant logs in order to attempt to determine the potential modus operandi associated with the cyber incident.				
ii.	Perform parsing & processing of collected logs and system artefacts.				
iii.	Subsequent forensic analysis and further co-relation, to identify the potential threat actors and outliers.				
iv.	Perform deep dive forensic analysis of identified systems, devices and systems and logs captured in the system.				
v.	Perform forensic fact-finding analysis of the incident with the objective to identify initial ingress point, egress points, lateral movement, and persistence of threat vectors, if any and identify the root cause of incident.				
vi.	Identify the malicious activities with respect to 5Ws + H (Why, When, Where, What, Who, How).				
vii.	Attempt, to the extent feasible identify the modus operandi of the attacker and determine if the attacker persisted in the Company network.				
viii.	Attempt, to the extent feasible the tools, tactics, techniques, and procedures (TTPs) adopted by the attacker.				
ix.	Identify and perform root cause analysis.				
x.	Perform evidence collection for legal and regulatory purposes. Bidder to ensure that acquisition performed should be acceptable in the court of law.				
xi.	Maintain Chain of Custody to Ensure evidence is securely stored and tracked at every step.				
xii.	Perform host, network, memory, and malware analysis; correlate across SIEM/EDR/NDR mapped to MITRE ATT&CK.				
xiii.	Analyze and report incidents based on severity				
C.	**Methodologies for handling of Cyber Incident and Response**				
i.	Prepare a draft assessment report and discuss findings with stakeholders. Deliver preliminary and final forensic reports, executive summaries, and regulatory support.				
ii.	No of entry points through which attackers can infiltrate into LIC network/systems.				
iii.	Collate the information obtained from different sources and submit a fact-finding Report.				
iv.	Remediation recommendations				
v.	Prepare a final fact-based report summarizing the outcomes of the work steps carried out and the information gathered from various sources.				

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.
This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted.

Signature of Bidder/Bidder's Representative

Date, Stamp and Seal of the Company