Selection of Service Provider for conducting Compromise Assessment and Incident Response Retainership
Annexure-D
Part-A: Compromise Assessment

CO-ERM-IT-CSD/2025-2026/CA & IRR dated 30th October, 2025

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 blue coloured cells.

Bidder's name	0

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

Annexure – D: Technical Scoring - Appendix D1 - Annual Turn Over in last Three financial years [i.e. 2022-2023, 2023-2024 and 2024-2025].

#	2022-2023	2023-2024	2024-2025	Evidence	Reference Page No.
Annual Turn Over in Crores					
Networth in Crores					

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 **Stamp and Seal** **Date**

Bidder's name	0

Selection of Service Provider for conducting Compromise Assessment
CO-ERM-IT-CSD/2025-2026/CA & IRR dated 30th October, 2025
Annexure – D: Technical Scoring - Appendix D2 - Letter of acceptance (LoA) /work order/ purchase order/ contract/

Name of Organization	Date of P.O/Contract	Start Date of Project	Project Duration in years	Value of P.O (INR)	Scope/Project details to be given as given above	No of Branches	Sector	Turnover of the Company in Crores	Evidence	Reference Page No.

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

Signature of Bidder/Bidder's Representative **Stamp and Seal** **Date:**

Bidder's name	0

Selection of Service Provider for conducting Compromise Assessment
CO-ERM-IT-CSD/2025-2026/CA & IRR dated 30th October, 2025
Annexure – D: Technical Scoring - Appendix D3 - Provide details of personnel.

#	Name of Resource	Name of Certification	Certification ID/No.	Certificate issuance date	Certificate Renewal Date	Total years of Experience	Reference Page No.(Copy of certificate to be
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							
31							
32							
33							

34							
35							
36							
37							
38							
39							
40							
41							
42							
43							
44							
45							

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

Signature of Bidder/Bidder's **Stamp and Seal of the Company**

Bidder's name	0

Selection of Service Provider for conducting Compromise Assessment and Incident Response Retainership
Annexure-D
Part-A: Compromise Assessment

CO-ERM-IT-CSD/2025-2026/CA & IRR dated 30th October, 2025
Annexure – D: Technical Scoring - Appendix D4 - Scope of Work

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
A.	**Immediate activities**				
A.(i)	Deployment of Solution: Solutions to be deployed to investigate systems from security point of view including applicable hardware and software infrastructure. Hardware will be provided by LIC in our private cloud infrastructure. RHEL and Mysql licenses will only be provided by LIC. All necessary software will be provided by the successful bidder.				
A.(ii)	Assessment of environment: Exhaustive library of Indicators of Compromise (IOC) and Threat Intelligence to be applied to evaluate network traffic, servers, desktops, network devices and critical log data for evidence of current and past malicious activities by following a grey box approach. Analysis will be conducted for endpoints (workstations, servers, laptops etc.), appliances, VPNs Cloud infrastructure, headless devices, databases, applications etc. which is a tentative list.				
A.(iii)	The category IOC list given is indicative but not exhaustive e.g. IOCs like file based, Network based, Registry based, process based, cloud, email etc.				
A.(iv)	Threat Feed and Threat Intel sources: vendors are required to have their own threat intelligence feeds integrated with commercial or open-source threat feeds (e.g., MISP, AlienVault OTX, Recorded Future, etc.) and Correlation with sector-specific or geopolitical IOCs (e.g., FIN7, APT29 (in BFSI or government).				
A.(v)	Analyze Evidence: Host and network forensic analysis as well as malware analysis to be performed to confirm the findings of the assessment in above mentioned activities. Detailed analysis required for this activity is given as a tentative list: Hashes of known malware (e.g., SHA256) Suspicious domain/IP connections Unauthorized use of admin tools (e.g., mimikatz, PsExec) Credential artifacts such as token theft or password dumping Persistence mechanisms (registry, scheduled tasks, WMI subscriptions) Abuse of scripting engines (e.g., PowerShell, WScript) Evidence includes (but is not limited to): • Indicators of Compromise (IOCs) like malicious IPs, domains, file hashes • Artifacts such as Suspicious processes, Abnormal registry entries, Unusual scheduled tasks • Suspicious user account activity • Logs such as Windows Event Logs, Linux syslogs, active directory logs, database logs, Firewall, proxy, VPN, DNS logs etc. • Network traffic captures (e.g., PCAP files) • Memory dumps or volatile memory artifacts • Authentication records (e.g., failed logins, lateral movement) • Cloud activity logs (IAM activity, object access) • Endpoint telemetry from EDR tools Analyzing logs and configurations to find traces of lateral movement, privilege escalation, or unauthorized access. Assessing each system's susceptibility to compromise through misconfigurations, unpatched vulnerabilities, or insecure practices.				
A. (vi)	Preventive Action: All findings with respect to security risks to be reported to LIC along with recommended action to contain the malicious actors and initiate preventive action.				
A. (vii)	Running comprehensive assessment on systems / devices from security perspective of the systems.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
A. (viii)	Assessment should detect all suspicious threat vectors on the systems / devices including but not limited to malwares, virus, Call back connections, Indicators of Compromise. This includes, but is not limited to: • Known and unknown malware (including in-memory and file less types) • Viruses, Trojans, and other malicious executable • Zero Day Attacks • Callback or command-and-control (C2) connections, including beaconing behavior • Relevant and contextual Indicators of Compromise (IOCs) such as suspicious file hashes, domain names, IP addresses, or registry changes • Signs of lateral movement, privilege escalation, and unauthorized persistence mechanisms • Anomalous user or system behavior that may indicate attacker presence The vendor is expected to leverage both signature-based detection and behavioral/threat hunting techniques, and provide detailed findings with appropriate evidence and risk classification. The detection methods should include: • Static and dynamic analysis of files and memory • Network traffic inspection for suspicious outbound connections • Correlation of telemetry from EDR, SIEM, firewall logs, and other available data sources • Retrospective hunting using historical logs or endpoint data				
B.	**Network Infrastructure**				
B. (i)	Review of core network architecture including placement of routers, switches, firewalls, servers, tools and network segmentation.				
B.(ii)	Review the adequacy of use cases defined to identify suspicious traffic, beaconing activity, and data exfiltration attempts.				
B.(iii)	Identify and document all potential entry points through which cyber attackers may gain access to the network.				
C.	**Endpoint Systems**				
C.(i)	Examination of a representative sample of servers, workstations, and laptops.				
C.(ii)	Deployment of endpoint detection tools or forensic agents (where applicable) to gather telemetry and logs.				
D.	**Identification of suspicious processes, services, scheduled tasks, or unauthorized tools**				
E.	**Active Directory and Identity Systems**				
E.(i)	Assessment of domain controllers and AD configuration for indicators of lateral movement or privilege escalation.				
E.(ii)	Review of user account behavior for anomalies (e.g., unusual login times, geographic anomalies).				
F.	**Email and Collaboration Platforms**				
F.(i)	Review of email gateway logs and inbox rules for potential business email compromise (BEC) or phishing indicators.				
F.(ii)	Analysis of other platforms for unauthorized access or mail forwarding rules.				
G.	**Cloud Infrastructure (if applicable)**				
G.(i)	Analysis of cloud workloads and storage buckets for misconfigurations or abnormal activity.				
G.(ii)	Review of audit logs, access control, and API usage.				
H.	**Threat Hunting and Intelligence Correlation**				
H.(i)	Correlation of internal telemetry with known threat actor tactics, techniques, and procedures (TTPs) from sources such as MITRE ATT&CK, threat intel feeds, and threat reports.				
H.(ii)	Use of YARA rules, IOC scanning, and anomaly detection tools to identify malicious artifacts.				
I	**Malware and Artifact Analysis**				
I (i)	Isolation and analysis of suspicious files or binaries found during the assessment.				
I (ii)	Reverse engineering of malware samples, if necessary, to understand capabilities and origin.				
J	**Remediation Recommendations**				
J (i)	Actionable guidance to remediate identified vulnerabilities, artifacts, and suspicious behavior.				
J (ii)	Best practices for improving detection and prevention capabilities.				
K	**IOC and TTP Report**				
K (i)	A list of indicators of compromise (IP addresses, domains, file hashes, etc.) found during the assessment.				
K (ii)	Mapping of TTPs to the MITRE ATT&CK framework where applicable.				
L	**Toolkits and Scripts**				
L (i)	Any scripts, YARA rules, or tools developed during the engagement for scanning or mitigation (if within scope).				
M	**Reports required (This is a tentative list but not exhaustive one)**				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
M (i)	a. Existing vulnerabilities and presence of IOCs, malware in servers, endpoint and network. b. Malware and persistence mechanisms c. Approach & methodology for conducting in-scope services. d. Relevant Experience through successful project highlights of similar nature. e. Hardware, software and license details to be provided f. Extensive library of Indicators of Compromise (IOC) and Threat Intelligence. g. References to 25 MITRE Attack. h. List of 50 Security Researchers, Analysts, and Incident Responders i. List of five (5) sample resumes that represent a typical team. Names of the individuals are not necessary. j. Details of Tools to be used k. Key Phases and Timelines to be demonstrated l. Your IOC collection and validation process m. Your threat intelligence sources n. How you ensure IOC relevance and freshness o. Demonstration of one assessment in line with the technical specification p. How IOCs are correlated across hosts, logs, and network q. Command and Control activities r. User account anomalies s. Data exfiltration and sabotage t. Detailed documentation of tools used and methodology employed u. System-wise/Device-wise exhaustive report of findings along with status v. IOCs / backdoor/ malicious software detected w. Executive summary				

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