REQUEST FOR PROPOSAL

For

SELECTION OF SERVICE PROVIDER FOR CONDUCTING CYBER SECURITY POSTURE ASSESSMENT

RFP Reference Number:

Ref: ECGC/Tender-14/RMD/07/2026-27

Dated: 14/08/2026

ECGC LIMITED

ECGC Bhawan, CTS No. 393, 393/1 to 45, M.V. Road, Andheri (East),

Mumbai-400069

Table of Contents

Section – 1

1. Introduction

1.1 Invitation to Bidders

By way of this Request for Proposal ('RFP') Document (hereinafter also referred to as 'the Bid Document' or 'the RFP Document') ECGC Limited (hereinafter referred to as 'ECGC / the Company'), a company wholly owned by Government of India and set up in 1957, invites competitive Bids on GeM portal from CERT-In empanelled firms/ consultants (hereinafter referred to as ('the Bidder(s)') for "**Conducting Cyber Security Posture Assessment**" as per scope of work and deliverables defined in Annexure – I of this RFP".

Prospective bidders are advised to check the prequalification criteria before applying for bids.

The Bidder(s) are advised to study the RFP Document carefully. Submission of Bids shall be deemed to have been done after careful study and examination of the RFP Document with full understanding of its terms, conditions, and implications.

Please note that all the required information asked needs to be provided. Incomplete information may lead to rejection of the Bid. The Company reserves the right to change the dates mentioned in this RFP Document at its sole discretion, which will be published on the Company's website/ GeM portal for information to the Bidders

1.2Schedule of events:

The various important dates relating to the RFP for **Selection of Service Provider for Conducting Cyber Security Posture Assessment** of ECGC is as under:

RFP Number	**ECGC/Tender-14/RMD/07/2026-27**
Mode of RFP	GeM
EMD	₹ 1,50,000/-
Date of Issue	14/08/2026

Last Date for submission of Pre-bid Queries (if any)	27/08/2026 up to 17:30P.M
Last date for submission of Bids	07/09/2026 up to 17:30P.M
Bid Opening date/ Opening of Date and Time for Eligibility Bids	07/09/2026
Date and Time for opening Financial Bids	15/09/2026
Contact Details: Deputy General Manager (RMD): Mr. Rajesh Joshi	
Telephone	022-66590532
All correspondence / queries relating to this RFP Document should be sent to following email ID only	rmd@ecgc.in

Note: Time lines are subject to change at the sole discretion of ECGC Ltd.

Any subsequent corrigendum/addendum to this RFP document, shall be published on the GeM portal and the Company's website www.ecgc.in. Prospective Bidders are requested to visit the website/GeM portal regularly.

Section - 2

Disclaimer

The information contained in this RFP Document or information provided subsequently to Bidder(s) in documentary form by or on behalf of ECGC, is provided to the Bidder(s) on the terms and conditions set out in this RFP Document and all other terms and conditions subject to which such information is provided, and the same shall be deemed to be a part of this RFP.

This RFP Document is neither an agreement nor an offer but is only an invitation by the Company to receive bids from interested and eligible bidders for **Conducting Cyber Security Posture Assessment** to assess emerging frontier AI driven cyber threats. No contractual obligation whatsoever shall arise from the RFP process until a formal contract is signed and executed by duly authorized signatories of ECGC and the selected bidder. ECGC reserves the right to cancel the entire process at any stage prior to the engagement of the consultant without any liability owed to any party.

The purpose of this RFP Document is to provide the Prospective Bidder(s) with information to assist the formulation of their bids. This RFP Document does not claim to contain all the information that each Bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information of this RFP document and where necessary obtain independent advices/clarifications. ECGC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

ECGC makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way for participation in this bidding process by bidders.

The Bidder is presumed to have examined all instructions, forms, terms and specifications in this RFP along with eligibility conditions as on the date of submission of its Bid. Failure to furnish all information required under this RFP or submission of a non-responsive bid in all respect will be at Bidder's risk and may result in rejection of the Bid.

This RFP is being issued with no financial commitment and ECGC reserves the right to reject any or all the bids / proposals received in response to this RFP document or withdraw the RFP at any stage without assigning any reason whatsoever and without any liability owed to any party whatsoever. The decision of ECGC in this regard shall be final, conclusive and binding on all the parties. The information provided by the Bidder in response to this RFP document will become the property of ECGC and will not be returned.

Section – 3

3. Instructions for Bidder(s)

3.1 General Instructions

3.1.1 ECGC expects a single bidder having in-house capabilities to deliver the scope as per the Scope of Work. Formation of consortium, joint venture or association of consultants or sub-contracting of services in whole or part with other firms shall not be permitted. In case the bidder is found to not possess the requisite capabilities, it will be summarily disqualified from the process of selection.

3.1.2 Bidder(s) shall submit their bid (comprising of "Eligibility/Technical" and "Financial" bid) online at GeM Portal. Bidders shall have to visit the GeM portal (http://gem.gov.in/), select the appropriate GeM bid number and upload electronically by scanning in PDF format duly filled and signed bid documents, defined forms. Bidders need to click on final submission link to submit their encrypted bid.

3.1.3 Prospective Bidders who have not enrolled/registered in GeM portal should enroll/register before participating through the website www.gem.gov.in

3.1.4 The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Company and supporting documents and printed literature shall be submitted in English.

3.1.5 The Bidder should ensure that there are no cuttings, over-writings, and illegible or undecipherable figures to indicate their Bid. All such Bids may be disqualified on this ground alone. The Bidder should ensure that ambiguous or unquantifiable costs/ amounts are not included in the Bid, which would disqualify the Bid.

3.1.6 The Bidder should commit to provide the resources desired by ECGC for the entire duration of the engagement, at the agreed cost and terms and conditions.

3.1.7 Partial Bids will not be accepted and shall stand rejected. Bidder(s) shall have to quote for the entire scope of work.

3.1.8 Bids not conforming to the requirements of the RFP may not be considered by ECGC. However, ECGC reserves the right at any time to waive any of the requirements of the RFP.

3.1.9 ECGC reserves the right to verify the validity and authenticity of bid information and reject any bid, where the contents/information are found incorrect/misrepresented whether partially or fully, at the time, during the process of RFP or even after award of the contract.

3.1.10 The bids once submitted cannot be modified or altered.

3.1.11 The Bidder shall bear all costs associated with the preparation and submission of its Bid, and ECGC will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the Bidding process.

3.1.12 It is clarified that GeM portal is used only as a platform for the RFP. All the terms and conditions contained in this RFP Document shall be applicable during the whole process.

3.2. Scope of Work

The detailed Scope of Work and timeline for deliverables are defined in Annexure – 1 of this RFP.

3.3. Pre-Bid Queries & Pre-Bid Meeting:

The Bidder(s) having any doubt/ queries/ concerns with any clause of this RFP document or selection process shall, before submission of their bids, raise their concern within the prescribed timelines specified in the "Schedule of Events" in Invitation to Bid. The queries shall be communicated only through the e-mail id provided, i.e., rmd@ecgc.in in the prescribed format (Annexure – 7). ECGC would issue clarifications/ Amendments in writing via e-mail or posting on company's website and will become part of RFP. The bidders are expected to use the opportunity to have all their queries answered. ECGC will not be liable to accept or provide any explanation towards any doubt/ concerns beyond the prescribed timeline.

A pre-bid meeting as per Schedule of Events given in the RFP document shall be held where bidders' queries will be discussed.

The bidders attending the pre-bid meeting shall compulsorily inform in advance about name, Designation, contact number (Mobile and Landline) of participants before the pre-bid meeting. Not more than 2 participants will be allowed from each bidder company.

3.4. Submission of bids

3.4.1. Online submission of bids: Online bids will have to be submitted as per Schedule of Events in the following manner: -

- **Eligibility and Technical Bid: Scanned Copies to be uploaded (.pdf):** The information should be prepared very carefully and as indicated in the RFP document, since it will form the basis for prequalification of bidder(s). Only relevant and to the point information /document should be uploaded. Failure to provide any required information, and accompanied documents supporting the eligibility criteria (as set out in Annexure-2) may lead to the rejection of the Bid. Bidder(s) must read the RFP document carefully before signing it. The following duly filled in annexures along with supporting documents shall be uploaded as part of Eligibility and Technical Bids:
    - Annexure – 2: Bidders' profile and Eligibility and applicable supporting documents as documentary evidence of eligibility;
    - Annexure-3 Technical Evaluation parameters
    - Annexure – 5: Acknowledgement;
    - Annexure – 8: Declaration;
    - Annexure – 10: Details of Professional staff;
    - Annexure – 11: Integrity Pact**;**

  Submission of financial quotation along with technical documents will be summarily rejected without further consideration.

- **Financial Bid (.pdf)**: Bidder(s) must read the terms and condition as mentioned in this RFP document and submit the form accordingly. Bidder(s) are required to check the prices / amount carefully before uploading financial bid. The following duly filled in annexures shall be uploaded as part of Financial Bid:
    - Annexure – 6: Financial Bid/Price Bid;

- Annexure – 4: Bank Details.

3.4.2. Non-submission of any of the specified documents by the bidder would result in rejection of bid. ECGC reserves the right to ask for additional/ alternate documents from the bidder. Only the bidders meeting the eligibility criteria will be taken forward to the next stage of Bidding process. The documentary evidence of the Bidder's qualifications to perform the Contract in its Bid will be accepted only if it is established that the same are to the Company's satisfaction.

3.4.3. The Bidder, for the purpose of making the Bid, shall complete the respective forms as annexed to the RFP document in all respects. No questions or items in the documents shall be left blank or unanswered. In case the bidder has no details or answers to be provided, a 'No' or 'Nil' or 'Not Applicable' or 'N.A.' statement shall have to be mentioned as appropriate. Bids documents with blank columns or unsigned forms will be summarily rejected.

3.4.4. The Bid shall be signed by a person or persons duly authorized by the Bidder with signature duly attested. In the case of a body corporate, the Bid shall be signed by the officers duly authorized by the body corporate with its common seal duly affixed. The Bidder shall affix its initials on each page of the Bid document.

3.4.5. **Professional Staff:** The bidder shall provide to ECGC a list of Professional Staff who shall work on the project along with their qualification and relevant experience in the format as provided under Annexure - 10. Bidder shall ensure that the same staff shall work on the project.

3.5. Bid Prices

3.5.1.1. All Prices are to be quoted in Indian Rupees only.

3.5.1.2. Prices quoted should be exclusive of all Central / State Government levies, taxes (including GST) and inclusive of all out-of-pocket expenses of the bidder. It may be noted that the ECGC will not pay any other amount and other

expenses like travel and accommodation etc. except the agreed professional fees and applicable taxes.

3.5.1.3. Prices quoted by the Bidder shall remain fixed during the Bidder's performance of the Contract if selected and shall not be subject to variation on any account, including exchange rate fluctuations excluding taxes/ duties/ levies/ cess, etc. which are subject to changes as per provisions of Central/State Government. A Bid submitted with an adjustable price quotation, other than exceptions specified herein, will be treated as non-responsive and shall be rejected.

3.6. Validity of Bids:

3.6.1. Bids shall remain valid for a minimum period of 90 days from the date of opening of the Bid. The prices quoted shall remain fixed and binding during the period of Contract unless agreed otherwise by the Company.

3.6.2. In exceptional circumstances, the Company may solicit the Bidder's consent to an extension of the period of validity of the Bid on the same terms and conditions. The request and the responses thereto shall be made in writing. At this point, a Bidder may refuse the request without risk of exclusion from any future RFPs or any debarment.

3.7. Evaluation of bids

3.7.1. The Company will examine the Bids pre-liminary to determine whether they are complete, whether the required formats have been furnished, the documents have been properly signed, whether the bid is responsive, i.e., conforms to all the terms and conditions of the RFP Document and that the Bids are generally in order. Non-responsive bids will be rejected summarily and the same may not be made responsive by correction of the non-conformity.

3.7.2. The Eligibility Evaluation will be conducted as per the criteria outlined in Annexure-2. Only those Bidders and Bids which have been found to be in conformity with the eligibility terms and conditions would be taken up by the Company for further detailed evaluation. The Bids which do not qualify the eligibility criteria and all terms during preliminary examination will not be taken up for further evaluation.

3.7.3. The incomplete Technical Bid will be subject to rejection. However, ECGC at its discretion may call for additional documents/ clarification from all bidders, if required.

3.7.4. The Bidders submitting bids and meeting the eligibility criteria will be invited for making presentation before the ECGC Technical Evaluation Committee for this RFP, and will be evaluated as per criteria specified in Technical Evaluation parameters (Annexure-3).

3.7.5. During evaluation and comparison of Bids, the Company may, at its discretion ask the Bidders for clarification of their bid or to provide additional documents. The request for clarification shall be in writing and no change in prices or substance of the Bid shall be sought, offered or permitted. No post Bid clarification at the initiative of the bidder shall be entertained. The bidders are expected to respond/provide the information/clarification within stipulated time. Failure to do so will lead to disqualification of the bidder.

3.8 Evaluation of Financial Bids/Price Bids and Finalization

i. 3.8.1 Financial Bids shall be opened for only those Bidders that are found eligible in the Technical Evaluation.

ii. 3.8.2. The Bids will finally be ranked on the basis of prices quoted with the lowest priced bid ranking highest. The final selection will be based on L1 criteria. Company may waive off any minor infirmity or non-conformity or irregularity in a Bid, which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.

3.9 Contacting the Company

3.9.1 No Bidder shall contact the Company on any matter relating to its Bid, from the time of opening of Financial Bid to the time the Contract is finalized and awarded.

3.9.2 Any effort by a Bidder to influence the Company in its decisions on Bid evaluation, bid comparison or contract award may result in the rejection of the said Bid and barring from any future RFPs / contracts / business with ECGC.

3.10. Performance Bank Guarantee

3.10.1. The successful Bidder (hereinafter referred to as the 'Vendor') shall be required to submit a Performance Bank Guarantee ("PBG") as per as Annexure-12 for a value equal to 3% of the Contract value (inclusive of applicable taxes) or equal to two quarters payment amount, valid for the period of the Contract (plus additional 8 weeks for claim period) from the date of satisfactory acceptance/ sign off by ECGC.

3.10.2. The PBG of contract value and validity period as mentioned above must be submitted within two weeks from the date of acceptance of the Letter of Award.

3.10.3. In case the contract period is extended beyond validity period due to nature of work, the PBG shall have to be extended/ renewed/ re-issued for the new/ extended contract period, including the claim period. The Vendor to make provisions for submission of extended PBG at least two weeks before the expiry of the original term of PBG in such case.

3.10.4. PBG shall be forfeited if the services are terminated abruptly by the Vendor or for any deviation by the Vendor from the terms of the Contract by way of which the Company can decide to forfeit the PBG. Further, unpaid charges, if any, will also not be paid in these circumstances. In case of no punitive action against the Vendor, the PBG (without any interest) will be returned after the 8 weeks from the satisfactory acceptance/ signoff by ECGC or on settlement of any claim against the Vendor, whichever is later.

3.11. Earnest Money Deposit

Earnest Money Deposit (EMD) of Rs.1,50,000 (One Lakh and Fifty Thousand only) is required to be submitted by NEFT/ RTGS mode only. The transaction details to be sent on rmd@ecgc.in along with following details,

Name of Bidder	
Date of EMD Transfer	
Unique Transaction reference (UTR)	
Beneficiary Name:	ECGC Limited

Bank Name:	Bank Of Baroda
Bank Account Number:	ECGCHEADZ
IFSC Code:	BARB0BANEAS (Fifth character is zero)
Bank Branch:	B K Complex, Mumbai
Bank Branch Address:	B 26 G Block, BKC, Bandra East, Mumbai 400051
PAN	AAACE0296K
GST	27AAACE0296K1ZJ
ECGC Address	ECGC Bhawan, CTS No. 393, 393/1-45, M.V. Road, Andheri (East), Mumbai, PIN 400069, Maharashtra, India

The transfer of the EMD amount needs to be completed along with submission of bid documents as per RFP Schedule of events 1.2 It is the bidder's responsibility to ensure timely transfer of the EMD. If the EMD is received after the designated date and time, the Company, at its discretion may reject the bid. EMD of unsuccessful Bidders shall be refunded within 30 days from the final result of the bidding process. EMD of successful bidder shall be refunded within 30 days post receipt of PBG without any interest. Under any circumstances, ECGC Ltd. will not be liable to pay any interest on the EMD. Offers made without the Earnest money deposit will be rejected. The amount of Earnest money deposit would be forfeited in the following scenarios:

a. In case the Bidder withdraws the bid prior to validity period of the bid without providing any satisfactory reason;

b. Amends its/his tender or impairs or derogates from the tender in any respect within the period of validity of the tender, or

c. In case the successful Bidder fails to provide the performance bank guarantee or sign the service agreement within specified period, without any satisfactory reason.

3.12 Award of Contract

3.12.1. The Bidder with the lowest price. i.e. L1 shall be awarded the Contract. ECGC will notify the successful Bidder in writing, by letter or by e-mail, that its Bid has been

accepted. The decision of ECGC shall be final, conclusive and binding on all the bidders/parties directly or indirectly connected with the bidding process. In case of tie - situation bidders having more number of experience in cyber security posture assessment in BFSI sector shall be given preference.

3.12.2. The notification of award will constitute the formation of the offer to contract. The selected Bidder should convey its intent of acceptance of the award of contract by returning a duly signed and stamped duplicate copy of the award letter within seven working days of receipt of the communication. If the selected bidder fails to enter into contract due to whatsoever reasons, ECGC will offer the Contract to the next qualified bidder/L2.

3.12.3. The selected Bidder shall have to execute a Contract i.e., the Service Agreement within 5 (five) working days of conveying acceptance and will be expected to commence the work as per 'Scope of Work'. The draft of the Service Agreement is enclosed and marked as Annexure – 9. ECGC reserves the right to alter / vary / amend / modify all or any of the terms and conditions set out in the said draft Agreement before its execution.

Section 4

ANNEXURE 1 - Scope of work

The Company proposes to carry out the Cyber Security Risk Posture Assessment in line with standard practices and frameworks such as Information Security Management System, BCMS, NIST, and evolving AI related threats covering the domains and activates/services included in the scope section.

The key activities to be performed as part of the engagement shall include but not be limited to the following:

- The successful bidder shall develop a detailed Cyber security posture assessment plan with appropriate project milestones based on the scope.
- The successful bidder shall undertake a comprehensive assessment of the entire Cyber Security Ecosystem including People, Processes, Technology, and Vendors that will include Information Security policies, sub-policies, procedures, business continuity plan, information and security controls, process, services, and associated guidelines and procedures operationalized in the Company.
- The Bidder should perform a comprehensive review of controls and control objectives already implemented and provide necessary recommendations for addition/ modification required in the existing controls implemented.
- The Bidder shall carry out the Technical Risk, Operational Risk, Cyber Risk related Assessment, and Testing activities to identify the areas of improvement in order to prepare the assurance report and maturity of the practices at the Company.
- The Bidder shall submit the report based on the gap assessment and propose remedial actions to fill the gap, assist team in mitigating those gaps and achieve conformance to the latest standard mapped with corresponding requirements as defined in NIST Cyber Security Framework, and other applicable Risk Management Standards.

Timelines:

- Project duration- 5-6 months

<u>Detailed Scope for Assessment, Gap Analysis, Recommendations and assistance for Addressing the Gaps</u>

1. Cyber Security Governance, Cyber Risk Management, and Cyber Security Compliance mechanisms

    a. Assessment of the Cyber Security Governance structure currently employed against global best practices and standards such as ISO 27001 and NIST framework, identify gaps in governance design, roles, responsibilities, and operating effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

    b. Review of Cyber Security Risk Assessment procedures, practices, and corresponding mitigation techniques, including frequency and methodology of risk assessments, and comparison against IRDAI 2026 Information Security Guidelines and CERT-In issued blueprints for reducing exposure and defending against AI-assisted vulnerability exploitation, identify gaps in risk management effectiveness and regulatory compliance, and provide actionable remediation guidance with support for implementation and closure verification.

    c. Review of all cyber security policy and procedure documents and compliance requirements from a regulatory perspective as well as global best practice standards, including data privacy frameworks, identify gaps in policy coverage, consistency, and regulatory alignment, and provide remediation recommendations with support for update, harmonization, and closure validation.

2. Cyber Asset Management

a. Review of Asset Inventory tools, practices, update mechanisms, review processes, and asset lifecycle management practices, identify gaps in completeness, accuracy, and governance of asset data, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. b. Assessment of asset version updates, patch updates, and other update practices and processes against applicable regulatory and CERT-In requirements, identify compliance and control gaps, and provide actionable remediation guidance with support for implementation planning and closure verification.

3. Cyber Vulnerability Management

a. Review of vulnerability assessment tools, practices, and processes employed within the Company, identify gaps in coverage, configuration, and effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Assessment of vulnerability identification workflows and associated processes to ensure compliance with relevant regulatory obligations and CERT-In requirements, including scenarios involving AI-assisted vulnerability discovery or exploitation, identify control and process gaps, and provide actionable remediation guidance with support for implementation and closure verification.

c. Integration of SBOM in the workflow

4. Patch Management

a. Review timelines between issuance of patches by vendors and application of patches, identify gaps/delays, and recommend corrective actions including support for remediation planning and closure tracking.

b. Review patch application practices and processes defined and used in the organization, identify process gaps, and assist in designing improvements and remediation actions to strengthen patch management maturity.

c. Review patch testing and approval processes to ensure compliance with regulatory obligations and CERT-In requirements, including resilience against AI-assisted vulnerability exploitation, and provide actionable remediation guidance with support for closure verification.

5. Configuration Management

a. Review of secure configuration benchmarking practices and processes, identify gaps in benchmark coverage, consistency, enforcement, and effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Review of processes for defining configuration benchmarks and associated automation mechanisms for benchmarking, identify gaps in benchmark definition methodology, automation maturity, and governance controls, and provide actionable remediation guidance with support for enhancement and closure verification.

c. Review of system hardening practices across all critical endpoints, identify gaps against baseline hardening standards and industry best practices, and provide remediation recommendations with support for strengthening controls and closure validation.

d. Review of processes for configuration benchmarks incorporating threat intelligence inputs and compliance with CERT-In and other applicable regulatory requirements as per latest 2026 guidelines, identify gaps in integration of threat intelligence, regulatory alignment, and update mechanisms, and provide remediation guidance with support for implementation and closure tracking.

6. Control Management

a. Review of risk-driven control management practices and processes against global best practices and standards, identify gaps in risk-to-control mapping, control design, implementation, and operating effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Review of configuration, policies, and effectiveness of security control processes and tools, including but not limited to Data Center & DR security controls, endpoint security, server security, Active Directory/DNS, VPN security, Wi-Fi security, MFA, perimeter security controls, cloud security preparedness, API security controls, DLP controls, and encryption/data security controls, identify gaps in design and operational effectiveness against regulatory requirements and industry best practices, and provide actionable remediation guidance with support for implementation and closure verification.

c. Review of control review mechanisms and hardening processes, identify gaps in control assurance processes, validation frequency, and hardening standards, and provide remediation recommendations along with support for strengthening control assurance and closure validation.

7. Continuous Monitoring, SOC Processes and Procedures

a. Review of the Company's SOC operations against industry best practices and applicable standards, identify gaps in SOC operating model maturity, processes, and governance effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Review of network monitoring, alert generation, and alert processing through workflow management systems, identify gaps in detection coverage, correlation logic, and workflow efficiency, and provide actionable remediation guidance with support for optimization and closure verification.

c. Review of endpoint monitoring, alert generation, and alert processing through workflow management systems, identify gaps in endpoint visibility, alert fidelity, and response workflows, and provide remediation recommendations with support for enhancement and closure validation.

d. Assessment of SIEM effectiveness, including use cases, correlation rules, and operational maturity, and review of readiness for future roadmap evolution towards SOAR adoption, identify gaps and provide a structured SIEM improvement and SOAR transition roadmap with remediation and implementation support.

e. Review of threat intelligence driven SOC operational practices and processes, identify gaps in ingestion, enrichment, and operational usage of threat intelligence, and provide remediation guidance with support for integration and closure tracking.

f. Review of digital forensics capabilities as part of incident response, including processes, tools, and skill levels, identify gaps in forensic readiness, tooling effectiveness, and skill maturity, and provide remediation recommendations with support for capability strengthening and closure verification.

g. Review of use of AI/ML in alert processing to enhance SOC analyst effectiveness, identify gaps in automation, model effectiveness, and operational integration, and provide remediation guidance along with roadmap recommendations for improvement and closure tracking.

h. Assessment of average turnaround time (TAT) in processing alerts, identify gaps in response efficiency and escalation workflows, and provide remediation recommendations to improve operational performance and closure tracking.

i. Review of training programs and skill levels of SOC operators, identify competency gaps and provide remediation recommendations including structured skill development plans and closure tracking mechanisms.

j. Review of efficacy of detecting malware and other intrusions through network monitoring systems, identify gaps in detection coverage, tuning, and response effectiveness, and provide remediation recommendations with support for enhancement and validation of improvements.

k. Review of incident response tools, processes, and practices, identify gaps in readiness, coordination, and tooling effectiveness, and provide remediation guidance with support for improvement and closure verification.

l. Review of incident response plans, identify gaps in completeness, regulatory alignment, and operational usability, and provide remediation recommendations with support for update and validation.

m. Review of cyber contingency plans, identify gaps in resilience planning, recovery objectives, and regulatory alignment, and provide remediation guidance along with support for enhancement and closure tracking.

n. Review of effectiveness of periodic cyber contingency and incident response drills, identify gaps in frequency, realism, coverage, and documentation, and provide remediation recommendations with support for strengthening exercise programs and closure validation.

o. Review of tabletop exercise practices, identify gaps in scenario coverage, stakeholder participation, and outcome tracking, and provide remediation guidance with support for maturity improvement and closure verification.

8. Ransomware Preparedness
    a. Review of Ransomware Detection and Mitigation Tools, Practices and Processes
    b. Review of Backup systems Efficacy and Security
    c. Backup Recovery processes, Practices and periodic Drills
    d. Ransomware Threat Intelligence Practices
9. Cloud Security - Frameworks, Solutions/services, and Processes, CSP, etc.
    a. Assessment of adaptability for private and public cloud infrastructure security posture checks to ensure adequate data security controls and reputation risk factors are addressed prior to transitioning to cloud environments, identify gaps in cloud security readiness, control design, and governance alignment, and provide remediation recommendations along with support for migration security planning and closure verification.
10. Third party and Vendor Risk Controls and Related Process Review
    a. Supply Chain Risk and Performance Management Process Review
11. Cyber Security Awareness and Skilling Practices
    a. Review of HR Security Practices Adequacy and Implementation to meet the security requirements.
    b. Processes of Training new employees as well as retraining and skilling employees periodically in cyber security awareness
12. In depth review of the Data Security and Privacy measures which support the business operations. The high-level review scope includes the following areas such as -
    - Use cases need to be considered including but not limited:
        - Possible data exfiltration attempt is detected by this alert.
        - Possible attempt to download a rootkit or exploit is detected by this use case.
        - User attempting to access malicious/blocked domain is detected with this alert.
        - Possible unauthorized successful connection is detected by this alert.

- A malicious process generating this traffic Possible C&C communication with domain or drive by Cyber Security Operation Centre and Related Support and Services

13. Secure Software Development Processes
    a. Review of DevSecOps practices, Processes, Tools and Skill Levels of Existing CI/CD pipeline engineers
    b. Review of Application Software Security Testing Tools, Processes and Capabilities

14. Red Team and Practices
    a. Review of Red Teaming processes, practices and skill levels
    b. VAPT Practices and Governance

15. Blue Team and Practices
    a. Review of Periodic Cyber Drills and Blue Team practices and skill levels
    b. Review of Process of learning from the drills to upgrade the capabilities
16. Review of the IT Infrastructure capacity/performance monitoring processes
17. Review of Authentication, Access Control and Remote Access Practices and Processes
    a. User Access Management and Identity Control Governance Processes

18. Review of the Company's Business Continuity Plan (BCP) and Disaster Recovery (DR) readiness against applicable regulatory requirements and industry best practices, identify gaps in business continuity and disaster recovery strategies, governance, processes, testing, and operational readiness, and provide actionable remediation recommendations with support for enhancement planning, implementation guidance, and closure verification.
19. Making Risk register and risk appetite statement aligned with IRDAI 2026 requirement
20. Assistance in fixing the gaps and re-drafting policy and procedure documents
21. Facility Level Physical & Environmental Security Controls processes

Approximate IT Infra and Apps details	Counts
Internal Ips	
External Ips	
Number of applications in scope.	
Endpoints are to be covered in DLP	
Number of vendors in scope	
IT User count	
Number of user locations	

Departments in scope:

I. Risk Management Department
II. Information Technology Department
III. Other - Human Resource Team, IT Infrastructure/Application Support Team, Accounts and Finance, Legal, Admin and Compliance & IRDA team.

Resource Requirement:

Bidder should ensure that resources are with minimum 5 plus years relevant experience having worked on at least 2 similar projects.

Project delivery and reports to be shared for both phases as below deliverables:

Sr. No.	Project Deliverables
1	Comprehensive Gap Assessment Report and Cyber Security Maturity Scorecard mapped to the NIST Cybersecurity Framework, Blueprint document of CERT-In guidance on AI-assisted cyber threats, and gap closure support by on ground team.
2	Cyber Security Risk Posture Dashboard
3	Management Report and Executive Presentation
4	Domain-wise Technical Control Assessment Reports
5	Three-Year Cyber Security Implementation Roadmap aligned with the NIST Cybersecurity Framework, clearly defining short-term (0–6 months), medium-term (6–18 months), and long-term (18–36 months) initiatives,
6	Enterprise Cyber Risk Register and Risk Appetite Statement,
7	Updated Cyber Security Governance Documentation, including revised and updated policies, standards, procedures, plans, and internal guidelines to address identified gaps
8	Implementation Assistance for a Next-Generation Security Operations Centre (SOC), including target operating model, architecture recommendations, technology roadmap, use-case development, implementation guidance, and support for aligning with IRDAI 2026 Information Security Guidelines, CERT-In guidance on AI-assisted cyber threats, and applicable DPDP Rules, 2025.
9	Cyber Security and Information Security Metrics Framework, including proposed Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), operational metrics, executive dashboards
Note: In addition to assistance in addressing identified gaps related to policy/configuration, rule changes, and tool efficiency assessments, Service provider has to provide ongound support in	

closing short-term requirements and a separate rate card requiring long-term implementation support of controls.

Annexure – 2 Eligibility Criteria

Specification	Complied (Yes/No)	Supporting Documents Required
The Bidder should be a partnership firm registered under LLP Act, 2008/Indian Partnership Act, 1932 or Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 and should have been in operation in India for last five years as on RFP date.		Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company (OR) Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies.
The Bidder must have an average turnover of minimum Rs.2.00 crore during last 03 (three) financial year(s) i.e. FY2023-24, FY 2024-25 and FY2025-26.		Copy of the audited financial statement for required financial years. (Certificate from statutory auditor for preceding/ 3 financial years may be submitted.)
The bidder should have at least 5 years experience in providing Cyber security posture assessment and support to BFSI sector out of which at least one PSU should be there.		The bidder should submit Satisfactory performance certificate from clients / Contract with client
The bidder shall have an established office and operational presence in Mumbai. All personnel deployed for the execution of this project shall be employees or authorized resources based		A suitable undertaking/or certificate or declaration by Bidder.

out of the bidder's Mumbai office and shall be available for on-site engagements at the Company's premises.		
Bidder should have a pool of minimum 05 professionals with certifications like OSCP, CISM,CISSP, CRTA,CISA and should be in permanent roster.		A suitable undertaking/or certificate or declaration by Bidder.
The Bidder must be familiar with and compliant with: 1. IRDAI Information Security guideline 2026 2. NIST Framework 3. Cert-In issued Blueprint document for AI assisted threats and defense strategies		Letter of confirmation from the Bidder.
The Bidder to provide information that any of its subsidiary or associate or holding company or companies having common director/s or companies in the same group of promoters/management or partnership firms/LLPs having common partners has not participated in the bid process.		Letter of confirmation from the Bidder.
Bidder should not be involved in any audit assignments of ECGC during past two years.		Letter of confirmation from the Bidder.
Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any State or Central Government or their agencies/ departments on the date of submission of bid for this EOI and also certify that they have not been disqualified		Letter of confirmation from the Bidder.

/ debarred / terminated on account of poor or unsatisfactory performance and/or blacklisted by any State or Central Government Agencies / Departments at any time, during the last 3 years.		

Annexure-3 Technical Evaluation Criteria

Technical bids will be subjected to following evaluation process. The eligible bidders will be required to give a presentation to ECGC for technical evaluation.

<table>
<tr><th>Sr. no.</th><th>Criteria Description</th><th colspan="2">Rules for awarding marks</th><th>Max. Marks</th></tr>
<tr><td>1.</td><td>No. of successfully completed/on-going assignments for cyber security posture assessment</td><td colspan="2">For each Completed-5 marks
For each on-going- 3 marks</td><td>15</td></tr>
<tr><td rowspan="6">2.</td><td rowspan="6">The number of OSCP, CISM,CISSP, CRTA,CISA or equivalent certified experienced personnel to be deployed in the ECGC project by the bidder. For each domain 5 marks will be awarded.</td><td>Certification/Qualification</td><td>Experience</td><td rowspan="6">25</td></tr>
<tr><td>CISA</td><td></td></tr>
<tr><td>CISSP</td><td></td></tr>
<tr><td>OSCP</td><td></td></tr>
<tr><td>CISM</td><td></td></tr>
<tr><td>Equivalent recognized certifications</td><td></td></tr>
<tr><td rowspan="2">3.</td><td rowspan="2">Experience in providing Cyber security maturity assessment to BFSI sector in last 3 years.</td><td colspan="2">More than or equal to 3- 10 marks</td><td rowspan="2">10</td></tr>
<tr><td colspan="2">Less than 3 -5 marks</td></tr>
<tr><td>4.</td><td>Presentation representing proposed project execution plan about the detailed approach/ methodology to be adopted for delivering the project deliverables.</td><td colspan="2">Points will be assigned by an internal committee based on the methodology, work plan, team composition and presentations. As per Table P-1</td><td>50</td></tr>
</table>

	It should also cover bidder's past experience & citations. (Maximum duration for presentation -45 minutes)		
Total			100

Bidders who score minimum of 60% marks on the technical evaluation criteria as mentioned above will only be considered for evaluation of commercial bid. The Commercial bids of the applicants with technical marks less than 60% will not be considered for commercial/financial evaluation.

Presentation of proposal:

ECGC will schedule the presentations and intimate the bidders of the date, time and locations. Failure of a bidder to complete a scheduled presentation may result in the rejection of that Bidder's proposal.

Table P-1

Sl. No.	Presentation Agenda	Marks
1	Detailed project execution plan	20
2	Past experience/client projects	10
3	Methodology and approach	15
4	Sample deliverables	5
Total		50

Annexure – 4

Bank Details of the Bidder

Sr No	Description	Details
1	Name of the Bank	
2	Address of the Bank	
3	Bank Branch IFSC Code	
4	Bank Account Number	
5	Type of Account	

.....

Signature of the authorized Signatory of Bidder

(Bidder's Seal)

Name:

Designation:

Contact No (Mobile)

Email Id

Annexure – 5

Acknowledgement

(To be submitted on the Bidder's letter head)

Date:

To,
The DGM(RMD)
ECGC Limited, 4th Floor, ECGC Bhawan,
CTS No. 393, 393/1 to 45,
M.V. Road, Andheri (East),
Mumbai-400069

Dear Sir/Madam,

Subject: Response to the Request for Proposal for conducting Cyber Security Posture Assessment

1. Having examined the RFP Document including Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide the services in accordance with the scope of work as stated in the RFP Document within the cost stated in the Bid.

2. If our Bid is accepted, we undertake to abide by all terms and conditions of this RFP document.

3. We certify that we have provided all the information requested by ECGC in the requested format. We also understand that ECGC has the right to reject this Bid if ECGC finds that the required information is not provided or is provided in a different format not suitable for evaluation process or complete information as necessitated

is not provided or for any other reason as it deems fit. ECGC's decision shall be final and binding on us.

4. We agree that ECGC reserves the right to amend, rescind or reissue this RFP Document and all amendments any time during the RFP process.

5. We agree that we have no objection with any of the clauses, terms and conditions and bidding process as provided in this RFP Document.

.....

Signature of the authorized Signatory of Bidder

(Bidder's Seal)

Name:

Designation:

Contact No (Mobile):

Email ID:

Annexure – 6

Price/Financial Bid for conducting Cyber Security Posture Assessment

We submit our financial bid (fees) for the proposed assignment as under:

Sr. No.	Description	Total Fees in INR (In Figures)
1.		

Total amount in words: Rupees_____only.

Terms & Conditions:

a. Payment of fee shall be in Indian Rupees only

b. No extra payment will be admissible other than fees quoted by the selected bidder in the financial bid. The fees quoted is **inclusive of all expenses**/costs/miscellaneous expenses, if any **but exclusive of all applicable taxes which shall be paid at actuals by ECGC Limited**. **ECGC Limited** would be entitled to deduct TDS as applicable while making payments according to the Indian taxation rules

c. The quoted rate is valid for entire tenure of the ensuing contract. No escalation on payment for this contract will be admissible.

d. Payment to be made as per terms of the Contract annexed herein and marked as Annexure 9.

e. No payment of any incidental and/or additional expenses, such as lodging, travelling, meals etc., in due course for execution of ensuing contract will be admissible.

f. No advance payment will be made on award of the contract.

Signature of the Authorized Signatory of Bidder

Name:

Designation:

Contact no. (Mobile):

Email Id:

Bidder's Seal:

Annexure –7

Queries Format

Sr No	Bidder Name	Page No. (RFP Ref)	Clause (RFP Ref)	Description in the RFP (RFP Ref)	Query
1					
2					

Note: The queries may be communicated only through the e-mail id provided is the Schedule of Events., Responses to the queries will be uploaded on ECGC website or emailed to concerned bidder. No queries will be accepted through telephone/ mobile or through any means other than in writing via e-mail. The queries shall be sent in .xls/.xlsx format in the above mentioned proforma.

Annexure – 8

DECLARATION FORMAT

(To be submitted on the Bidder's letter head)

DECLARATION

I_____son of Shri_____working as _____in_____(name of the Bidder and address in full be mentioned), hereby solemnly affirm and declare that I have been authorized by the firm to sign the Bid & related documents. I, hereby declare and certify, on behalf of the firm, that we have accepted all the terms & conditions mentioned in this RFP document and we shall abide by all the terms & conditions of the RFP in the event of acceptance of my/our Bid.

I further declare that M/s._____(Name of the Bidder)/ any of its partners/relatives/employees/representatives/agents shall not, under any circumstances, be deemed to have any employer-employee relationship with ECGC Ltd. / ECGC Ltd. Officials. I also declare that I/We do not possess any place of profit in ECGC Ltd. I declare that our firm is/was not under default/ prohibited/debarred/blacklisted by any regulating authority/agency including but not limited to IRDAI, RBI, SEBI, ICAI, CAG, IAI etc.

I also declare that none of the ECGC Ltd. officials, employees of ECGC Ltd. have any vested and personal interest in the Bidding firm. I undertake to sign Service Agreement with ECGC Ltd. on behalf of our Firm if selected as successful bidder and on acceptance of Award Letter as per Draft in Annexure-8 attached in the RFP.

I declare that all information submitted by me is true and correct to the best of my knowledge. I/We have no objection if any enquiries are made about my work/clients listed by me/us.

I/We declare that I/we have read all the terms & conditions of bid and the instructions and they are acceptable to me/us. We further declare to abide by the same.

I/ We Confirmation that I/We are not associated with the ECGC Ltd. on any cyber security assignment during the period of FY 2024-25 and shall not be associated with ECGC Ltd. on any cyber audit assignment during the period of FY 2025-2026.

Signature of Authorized Signatory

Stamp

Place:_____ Dated: _____

Name:_____ Designation:_____

Annexure – 9

DRAFT SERVICE AGREEMENT

(To be submitted by the Successful Bidder after acceptance of Letter of Award)

This **SERVICE AGREEMENT** ("**Agreement**") is made and entered into on this the [•] day of [•] Two Thousand and Twenty-Six [___/[___]/2026) at (Place), BY AND BETWEEN:

ECGC Ltd., a Central Public Sector Enterprise wholly owned by the Government of India, having its registered office at ECGC Bhawan, CTS No. 393, 393/1 to 45, M.V. Road, Andheri (East), Mumbai-400069 (hereinafter referred to as the "**Company**", which term shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors-in-interest and permitted assigns), of the ONE PART;

AND

_____, a company incorporated under the Indian Companies Act, 1956/2013 or a firm registered under LLP Act, 2008/Indian Partnership Act, 1932, having its registered office at ' -- '(hereinafter referred to as the "**Service Provider**", which term shall, unless repugnant to the context or meaning thereof, be deemed to mean and include its successors-in-interest and permitted assigns), of the OTHER PART.

Company and the Service Provider shall hereinafter jointly be referred to as "Parties" and individually as a "Party"

WHEREAS:

1. The Company is, *inter alia*, engaged in the business of providing export credit insurance to Indian exporters and Banks;

2. The Service Provider is a service organization empaneled by the Indian Computer Emergency Response Team (CERT-In) under the Department of Electronics & IT, for conducting cyber security posture assessment, including vulnerability assessment and penetration testing of computer systems, networks, computer resources & applications of various agencies or departments of the Government, *inter alia*, involved in the business of providing Cybersecurity Services.

3. The Company floated a Request For Proposal (RFP) having reference: **ECGC/Tender-14/RMD/07/2026-27** (hereinafter referred to as "the said RFP") (Attached as Annexure – p to this Agreement).

4. The Service Provider participated in the RFP and submitted its Bid response dated [_____] in response to the RFP, representing that as a CERT-In empanelled organization, it possesses the necessary professional expertise for **CONDUCTING CYBER SECURITY POSTURE ASSESSMENT** and agrees to fully comply the "Guidelines for CERT-In Empaneled Organizations, Terms & conditions of empanelment and Policy guidelines for handling related data" while conducting Cyber Security posture assessment.

5. Based on the Bid evaluation, the Service Provider has become the successful bidder in the said RFP and the Company has selected the Service Provider to conduct Cyber Security Posture Assessment and the Service Provider has agreed to provide the services, as they have the required skills and personnel.

NOW THEREFORE, in consideration of the mutual covenants, terms and conditions and understandings set forth in this Agreement, the Parties with the intent to be legally bound hereby agree as follows:

1. Definitions:

In this Contract, the following terms shall be interpreted as indicated:

i. "Service Provider" is the successful Bidder and to whom notification of award has been given by ECGC.

ii. "The Services" means the scope of services which the Service Provider is required to provide ECGC under the Contract.

iii. “The Contract” means this agreement entered into between ECGC and the Service Provider, and signed by the parties, including all annexures, attachments and appendices thereto and all documents incorporated by reference therein and any subsequent amendments executed in writing by both Parties.

iv. “The Contract Price” means the price payable to the Service Provider under the Contract for the full and proper performance of its contractual obligations;

v. “TCC” means the Terms and Conditions of Contract;

vi. “The Project/assignment” means conducting Cyber Security Posture Assessment as per the Scope of Work.

vii. Confidential Information means all the information of the Company which is disclosed to the service provider whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, techniques, processes, plans, algorithms, software programs, source code, business methods, customer lists, contacts, financial information, sales and marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs, operations, strategies, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription lists, customer lists, photo files, advertising materials, contract quotations, charity contracts, documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, statistics, facts, figures, numbers, records, professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barristers, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors,

Surveyors, Loss Assessors, Investigators, Forensic experts, Scientists, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Bhartiya Sakshya Adhiniyam, 2023, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defences taken before a Court of Law, Judicial Forum, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Company.

2. Appointment & Scope Of Work

a. The Company hereby appoints the Service Provider to provide the 'Services' clearly set out under the '**Scope of Work** as given below:

The key activities to be performed as part of the engagement shall include but not be limited to the following:

- The successful bidder shall develop a detailed Cyber security posture assessment plan with appropriate project milestones based on the scope.
- The successful bidder shall undertake a comprehensive assessment of the entire Cyber Security Ecosystem including People, Processes, Technology, and Vendors that will include Information Security policies, sub-policies, procedures, business continuity plan, information and security controls, process, services, and associated guidelines and procedures operationalized in the Company.
- The Bidder should perform a comprehensive review of controls and control objectives already implemented and provide necessary recommendations for addition/ modification required in the existing controls implemented.
- The Bidder shall carry out the Technical Risk, Operational Risk, Cyber Risk related Assessment, and Testing activities to identify the areas of improvement

in order to prepare the assurance report and maturity of the practices at the Company.

- The Bidder shall submit the report based on the gap assessment and propose remedial actions to fill the gap, assist team in mitigating those gaps and achieve conformance to the latest standard mapped with corresponding requirements as defined in NIST Cyber Security Framework, and other applicable Risk Management Standards.

Timelines:

- Project duration- 5-6 months

Detailed Scope for Assessment, Gap Analysis, Recommendations and assistance for Addressing the Gaps

22. Cyber Security Governance, Cyber Risk Management, and Cyber Security Compliance mechanisms

    a. Assessment of the Cyber Security Governance structure currently employed against global best practices and standards such as ISO 27001 and NIST framework, identify gaps in governance design, roles, responsibilities, and operating effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

    b. Review of Cyber Security Risk Assessment procedures, practices, and corresponding mitigation techniques, including frequency and methodology of risk assessments, and comparison against IRDAI 2026 Information Security Guidelines and CERT-In issued blueprints for reducing exposure and defending against AI-assisted vulnerability exploitation, identify gaps in risk management effectiveness and regulatory compliance, and provide actionable remediation guidance with support for implementation and closure verification.

c. Review of all cyber security policy and procedure documents and compliance requirements from a regulatory perspective as well as global best practice standards, including data privacy frameworks, identify gaps in policy coverage, consistency, and regulatory alignment, and provide remediation recommendations with support for update, harmonization, and closure validation.

23. Cyber Asset Management

a. Review of Asset Inventory tools, practices, update mechanisms, review processes, and asset lifecycle management practices, identify gaps in completeness, accuracy, and governance of asset data, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. b. Assessment of asset version updates, patch updates, and other update practices and processes against applicable regulatory and CERT-In requirements, identify compliance and control gaps, and provide actionable remediation guidance with support for implementation planning and closure verification.

24. Cyber Vulnerability Management

a. Review of vulnerability assessment tools, practices, and processes employed within the Company, identify gaps in coverage, configuration, and effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Assessment of vulnerability identification workflows and associated processes to ensure compliance with relevant regulatory obligations and CERT-In requirements, including scenarios involving AI-assisted vulnerability discovery or exploitation, identify control and process gaps, and provide actionable remediation guidance with support for implementation and closure verification.

c. Integration of SBOM in the workflow

25. Patch Management

a. Review timelines between issuance of patches by vendors and application of patches, identify gaps/delays, and recommend corrective actions including support for remediation planning and closure tracking.

b. Review patch application practices and processes defined and used in the organization, identify process gaps, and assist in designing improvements and remediation actions to strengthen patch management maturity.

c. Review patch testing and approval processes to ensure compliance with regulatory obligations and CERT-In requirements, including resilience against AI-assisted vulnerability exploitation, and provide actionable remediation guidance with support for closure verification.

26. Configuration Management

a. Review of secure configuration benchmarking practices and processes, identify gaps in benchmark coverage, consistency, enforcement, and effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Review of processes for defining configuration benchmarks and associated automation mechanisms for benchmarking, identify gaps in benchmark definition methodology, automation maturity, and governance controls, and provide actionable remediation guidance with support for enhancement and closure verification.

c. Review of system hardening practices across all critical endpoints, identify gaps against baseline hardening standards and industry best practices, and provide remediation recommendations with support for strengthening controls and closure validation.

d. Review of processes for configuration benchmarks incorporating threat intelligence inputs and compliance with CERT-In and other applicable

regulatory requirements as per latest 2026 guidelines, identify gaps in integration of threat intelligence, regulatory alignment, and update mechanisms, and provide remediation guidance with support for implementation and closure tracking.

27. Control Management

    a. Review of risk-driven control management practices and processes against global best practices and standards, identify gaps in risk-to-control mapping, control design, implementation, and operating effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

    b. Review of configuration, policies, and effectiveness of security control processes and tools, including but not limited to Data Center & DR security controls, endpoint security, server security, Active Directory/DNS, VPN security, Wi-Fi security, MFA, perimeter security controls, cloud security preparedness, API security controls, DLP controls, and encryption/data security controls, identify gaps in design and operational effectiveness against regulatory requirements and industry best practices, and provide actionable remediation guidance with support for implementation and closure verification.

    c. Review of control review mechanisms and hardening processes, identify gaps in control assurance processes, validation frequency, and hardening standards, and provide remediation recommendations along with support for strengthening control assurance and closure validation.

28. Continuous Monitoring, SOC Processes and Procedures

    a. Review of the Company's SOC operations against industry best practices and applicable standards, identify gaps in SOC operating model maturity, processes, and governance effectiveness, and provide remediation recommendations along with support for improvement planning and closure tracking.

b. Review of network monitoring, alert generation, and alert processing through workflow management systems, identify gaps in detection coverage, correlation logic, and workflow efficiency, and provide actionable remediation guidance with support for optimization and closure verification.

c. Review of endpoint monitoring, alert generation, and alert processing through workflow management systems, identify gaps in endpoint visibility, alert fidelity, and response workflows, and provide remediation recommendations with support for enhancement and closure validation.

d. Assessment of SIEM effectiveness, including use cases, correlation rules, and operational maturity, and review of readiness for future roadmap evolution towards SOAR adoption, identify gaps and provide a structured SIEM improvement and SOAR transition roadmap with remediation and implementation support.

e. Review of threat intelligence driven SOC operational practices and processes, identify gaps in ingestion, enrichment, and operational usage of threat intelligence, and provide remediation guidance with support for integration and closure tracking.

f. Review of digital forensics capabilities as part of incident response, including processes, tools, and skill levels, identify gaps in forensic readiness, tooling effectiveness, and skill maturity, and provide remediation recommendations with support for capability strengthening and closure verification.

g. Review of use of AI/ML in alert processing to enhance SOC analyst effectiveness, identify gaps in automation, model effectiveness, and operational integration, and provide remediation guidance along with roadmap recommendations for improvement and closure tracking.

h. Assessment of average turnaround time (TAT) in processing alerts, identify gaps in response efficiency and escalation workflows, and provide

remediation recommendations to improve operational performance and closure tracking.

i. Review of training programs and skill levels of SOC operators, identify competency gaps and provide remediation recommendations including structured skill development plans and closure tracking mechanisms.

j. Review of efficacy of detecting malware and other intrusions through network monitoring systems, identify gaps in detection coverage, tuning, and response effectiveness, and provide remediation recommendations with support for enhancement and validation of improvements.

k. Review of incident response tools, processes, and practices, identify gaps in readiness, coordination, and tooling effectiveness, and provide remediation guidance with support for improvement and closure verification.

l. Review of incident response plans, identify gaps in completeness, regulatory alignment, and operational usability, and provide remediation recommendations with support for update and validation.

m. Review of cyber contingency plans, identify gaps in resilience planning, recovery objectives, and regulatory alignment, and provide remediation guidance along with support for enhancement and closure tracking.

n. Review of effectiveness of periodic cyber contingency and incident response drills, identify gaps in frequency, realism, coverage, and documentation, and provide remediation recommendations with support for strengthening exercise programs and closure validation.

o. Review of tabletop exercise practices, identify gaps in scenario coverage, stakeholder participation, and outcome tracking, and provide remediation guidance with support for maturity improvement and closure verification.

29. Ransomware Preparedness

    a. Review of Ransomware Detection and Mitigation Tools, Practices and Processes

    b. Review of Backup systems Efficacy and Security

    c. Backup Recovery processes, Practices and periodic Drills

    d. Ransomware Threat Intelligence Practices

30. Cloud Security - Frameworks, Solutions/services, and Processes, CSP, etc.

    a. Assessment of adaptability for private and public cloud infrastructure security posture checks to ensure adequate data security controls and reputation risk factors are addressed prior to transitioning to cloud environments, identify gaps in cloud security readiness, control design, and governance alignment, and provide remediation recommendations along with support for migration security planning and closure verification.

31. Third party and Vendor Risk Controls and Related Process Review

    a. Supply Chain Risk and Performance Management Process Review

32. Cyber Security Awareness and Skilling Practices

    a. Review of HR Security Practices Adequacy and Implementation to meet the security requirements.

    b. Processes of Training new employees as well as retraining and skilling employees periodically in cyber security awareness

33. In depth review of the Data Security and Privacy measures which support the business operations. The high-level review scope includes the following areas such as -

    - Use cases need to be considered including but not limited:
        - Possible data exfiltration attempt is detected by this alert.
        - Possible attempt to download a rootkit or exploit is detected by this use case.
        - User attempting to access malicious/blocked domain is detected with this alert.
        - Possible unauthorized successful connection is detected by this alert.

- A malicious process generating this traffic Possible C&C communication with domain or drive by Cyber Security Operation Centre and Related Support and Services

34. Secure Software Development Processes
    a. Review of DevSecOps practices, Processes, Tools and Skill Levels of Existing CI/CD pipeline engineers
    b. Review of Application Software Security Testing Tools, Processes and Capabilities

35. Red Team and Practices
    a. Review of Red Teaming processes, practices and skill levels
    b. VAPT Practices and Governance

36. Blue Team and Practices
    a. Review of Periodic Cyber Drills and Blue Team practices and skill levels
    b. Review of Process of learning from the drills to upgrade the capabilities
37. Review of the IT Infrastructure capacity/performance monitoring processes
38. Review of Authentication, Access Control and Remote Access Practices and Processes
    a. User Access Management and Identity Control Governance Processes

39. Review of the Company's Business Continuity Plan (BCP) and Disaster Recovery (DR) readiness against applicable regulatory requirements and industry best practices, identify gaps in business continuity and disaster recovery strategies, governance, processes, testing, and operational readiness, and provide actionable remediation recommendations with support for enhancement planning, implementation guidance, and closure verification.
40. Making Risk register and risk appetite statement aligned with IRDAI 2026 requirement
41. Assistance in fixing the gaps and re-drafting policy and procedure documents
42. Facility Level Physical & Environmental Security Controls processes

Approximate IT Infra and Apps details	Counts
Internal Ips	
External Ips	
Number of applications in scope.	
Endpoints are to be covered in DLP	
Number of vendors in scope	
IT User count	
Number of user locations	

Departments in scope:

IV. Risk Management Department
V. Information Technology Department
VI. Other - Human Resource Team, IT Infrastructure/Application Support Team, Accounts and Finance, Legal, Admin and Compliance & IRDA team.

Resource Requirement:

Bidder should ensure that resources are with minimum 5 plus years relevant experience having worked on at least 2 similar projects.

Project delivery and reports to be shared for both phases as below deliverables:

Sr. No.	Project Deliverables
1	Comprehensive Gap Assessment Report and Cyber Security Maturity Scorecard mapped to the NIST Cybersecurity Framework, Blueprint document of CERT-In guidance on AI-assisted cyber threats, and gap closure support by on ground team.
2	Cyber Security Risk Posture Dashboard
3	Management Report and Executive Presentation
4	Domain-wise Technical Control Assessment Reports
5	Three-Year Cyber Security Implementation Roadmap aligned with the NIST Cybersecurity Framework, clearly defining short-term (0–6 months), medium-term (6–18 months), and long-term (18–36 months) initiatives,
6	Enterprise Cyber Risk Register and Risk Appetite Statement,
7	Updated Cyber Security Governance Documentation, including revised and updated policies, standards, procedures, plans, and internal guidelines to address identified gaps
8	Implementation Assistance for a Next-Generation Security Operations Centre (SOC), including target operating model, architecture recommendations, technology roadmap, use-case development, implementation guidance, and support for aligning with IRDAI 2026 Information Security Guidelines, CERT-In guidance on AI-assisted cyber threats, and applicable DPDP Rules, 2025.
9	Cyber Security and Information Security Metrics Framework, including proposed Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), operational metrics, executive dashboards
Note: In addition to assistance in addressing identified gaps related to policy/configuration, rule changes, and tool efficiency assessments, Service provider has to provide ongound support in closing short-term requirements and a separate rate card requiring long-term implementation support of controls.	

Here to with effect from …… ("**Effective Date**") and the Service Provider hereby agrees to provide the Services in accordance with the terms and conditions set out below.

b. The Service Provider, acting as an independent contractor, shall provide the Services ("**Services**") and the Deliverables ("**Deliverables**"), if any, as more particularly set out in **Scope of Work** hereto.

c. The **Scope of Work** shall specify the Services, which shall include, but shall not be limited to, applicable fees, term or duration for which Services shall be provided, specifications, service levels, and project timelines, as well as any requirements that are in addition to this Agreement, such as specific project milestones, acceptance criteria or other quality and warranty considerations. The Statement of Work shall further delineate the rights, duties, and obligations of the Parties related to the particular Service.

3. Payment Terms and Milestones

a. Payment shall be made in Indian Rupees.
b. Payment shall be made via electronic fund transfer only to the bank account provided as per the form under Annexure -8 to the RFP response.
c. No payment shall be made in advance on award of the contract.
d. Payments shall be made only on receipt of invoice from the Service Provider, after completion of the Scope of Work to the satisfaction of ECGC Limited.
e. It may be noted that ECGC shall not pay any amount / expenses / charges/ fees / travelling expenses / boarding expenses / lodging expenses / conveyance expenses / out of pocket expenses etc. other than the agreed amount as per the contract.
f. The fees payable for the Services provided herein and the terms and procedure for payments thereof are set forth in the relevant **Scope of Work**.
g. The price mentioned are exclusive of all the taxes and duties as applicable, which shall be borne by the Company at actuals as on the date of invoice.
h. All payments shall be subject to TDS and any other taxes as per the tax rules prevalent at the time of payment.
i. All the payments would be against the submission of the invoices to the Company along with the relevant supporting documents, if any.

j. All invoices shall be paid within 30 days from the date of receipt or as per the payment terms agreed in the relevant **Scope of Work**.

k. Payment Milestone: Payment will be released after receiving all the deliverables as per Scope of work.

4. Service Provider's Responsibilities

The Service Provider shall be responsible for:

i. providing the materials (if any), documentation, analysis, data programs and Services to be delivered or rendered hereunder, of the type and quality as specified in the relevant **Scope of Work.**

ii. Complying with Company's internal guidelines, instructions, manuals, scrutiny lists, procedures, further specifics and requirements ("**Guidelines**") in relation to the Services, as may be provided in writing by the Company to the Service Provider. However, in the event there is a conflict between the guidelines and the terms set out in the Agreement, the terms set out in the Agreement shall prevail;

iii. Supervising and controlling its personnel deployed (If any) at the Company's premises for providing the Services; and

iv. Complying with all applicable laws in the course of providing the Services.

v. Any other responsibilities that may arise during the performance of the services as mentioned in **Scope of Work**.

5. Company's Responsibilities

The Company, on its part, shall be responsible for:

i. Providing the necessary assistance for delivery of Services at offsite or at its premises including by way of providing the necessary equipment, media, supplies and such other facilities as set out in relevant **Scope of Work**.

ii. Ensuring the security and safety of the Service Provider's personnel and Service Provider Equipment, deployed at the Company's premises;

iii. Providing access to the Service Provider's personnel to the different parts of the Company's premises, personnel and various systems of the

Company, including computers, servers, networks as may be required for the purpose of providing the Services;

iv. Ensuring that all policies and procedures of the Service Provider are complied with in the course of availing of the Services;

v. Performing all other general acts as may be necessary to enable the Service Provider to efficiently provide the Services.

6. Service Delivery Location

The major scope of work as mentioned above will be required to be delivered at ECGC's onsite location at ECGC Bhawan, CTS No. 393, 393/1 to 45, M.V. Road, Andheri (East), Mumbai-400069. The Team would be required to travel and / or be posted at ECGC's Data Centre Site in Mumbai for work-related matters. The Team may also be required to travel for meetings with / discussions with / presentations to the different departments of ECGC as per scope of work. The Team may also visit the existing Data Centre and Disaster Recovery locations of ECGC to ascertain the inputs required for drawing out the specifications, if required.

7. Intellectual property

a. All the manuals, guidelines, documents etc. provided by Company shall be treated as Confidential information by the Service Provider.

b. Service Provider shall retain all rights, title, interest including intellectual rights in and to the methodologies, procedures, techniques, ideas, concepts etc. embodied in the deliverables, developed or supplied in connection with this Agreement.

c. The Service Provider shall provide Reports, Documents and all other relevant materials, artefacts etc. during the assignments to ECGC Ltd. and ECGC Ltd. shall own all IPRs in such Reports, Documents and all other relevant materials, artefacts etc. All documents related to such shall be treated as confidential information by the Bidder.

d. Any royalties or patents or the charges for the use or infringement thereof that may be involved in the contract shall be included in the price. Service Provider shall protect ECGC against any claims thereof.

e. It is however hereby clarified that if the Deliverables incorporate any pre-existing intellectual property rights of the Company the rights therein shall continue to vest with the Company.

f. For the sake of clarity parties agree and specifically provide that the Service Provider shall retain full rights and ownership of all Service Provider Certifications, Service Provider Software / Products, including any new release (s) and upgrade(s) thereof

g. A party shall not directly or indirectly, use any of the other party's trademarks, trade names, service marks and logos in any manner, except as permitted by the other party in writing.

8. Confidentiality & Personal Data obligations:

a. The Company shall be deemed to be the owner of all Confidential Information.

b. The Service Provider acknowledges that it will have access to sensitive, proprietary, and personal data belonging to ECGC, its clients, and Indian citizens. The service provider will use the Confidential Information solely to fulfil its obligations as part of and in furtherance of this service contract.

c. The Service provider shall keep strictly confidential all information received, accessed, or created in connection with its engagement with the Company, including but not limited to technical, operational, strategic, business, employee, customer, and financial information, whether oral, written, electronic or otherwise ("Confidential Information"). This includes any "Personal Data" as defined under the Digital Personal Data Protection Act, 2024 ("DPDP Act").

d. The Service provider shall not disclose such Confidential Information to any third party without the prior written consent of the Company, except to those who need to know it for the execution of their duties and are bound by similar obligations of confidentiality.

e. The Service provider understands that Confidential Information shall be used solely for the purposes of fulfilling responsibilities under this assignment. Unauthorized use, duplication, or disclosure of any Confidential Information for personal or third-party benefit is strictly prohibited.

f. The Service provider shall

   i. Process Personal Data strictly as per the Company's instructions and for the lawful purpose communicated by the Company.

ii. Ensure full compliance with the provisions of DPDP Act and its rules, ECGC's procedures and policies in place with respect to DPDP, Standard cybersecurity guidelines issued by RBI and CERT-In, and any other applicable data protection laws.

iii. Implement appropriate technical and organizational safeguards to protect against unauthorized access, loss, misuse, or disclosure of Personal Data.

iv. Promptly notify the Company of any actual or suspected data breach involving Personal Data.

v. Destroy or return any Personal Data or Confidential Information upon the conclusion of the engagement or on written instructions from the Company, except where retention is legally mandated.

vi. Indemnify and hold the Company harmless against any claims, losses, damages, expenses (including legal fees), or liabilities arising out of or in connection with any breach of confidentiality and data protection obligations.

g. Notwithstanding the termination or completion of the assignment, the provisions relating to indemnification, confidentiality of information, and protection of personal data, including all obligations arising under applicable laws such as the DPDP Act and its rules, shall survive and continue to remain binding upon the Vendor. All rights and remedies hereunder are cumulative and in addition to any other rights or remedies under any applicable law, at equity, or under this Agreement, subject only to any limitations stated herein.

9. Penalty

The company reserves the right to deduct from the total contract price to be paid to the Service Provider in such manner in the event of the following:

Reason	Delay of One Week	Delay beyond One week and part thereof
Delay in Providing /ensuring deliverables / services beyond the agreed timeline (delay attributable to the service provider)	Caution Note	5% of the contract value, and proportionally for the part of the week. Minimum 5%

Inordinate delay in responding to the references made by the company (delay attributable to the service provider)	Caution Note	5% of the contract value, and proportionally for the part of the week. Minimum 5%

10. Indemnity and Limitation of Liability

a. Defaulting party shall indemnify, defend and hold harmless the other from and against any and all liability, losses, costs and expenses (including reasonable attorney's fees) relating to or arising out of the breach of this Agreement, the negligence or willful misconduct of defaulting party, or its employees or agents. No party shall however be liable for any loss or damage arising from reliance on any information or materials supplied by the other party or any third party on behalf of the other party, or for any inaccuracy or other defect in any information or materials supplied by the other party or any third party on behalf of the other party.

b. Notwithstanding anything stated herein, neither party shall be liable to the other party for any indirect, incidental, consequential, special or exemplary or other damages, including but not limited to loss of business, profits, information, business interruption and the like, suffered by the other or any third party under or in pursuance of the terms hereof, howsoever arising, whether under contract, tort or otherwise, even if advised about the possibility of the same.

c. Except for breach of Confidentiality and Infringement of Intellectual property rights under this agreement, each party's total aggregate liability for any damages, losses, costs, liabilities arising out of or in connection with this Agreement whether under contract, tort or otherwise shall not exceed an amount equivalent to the total contract value.

d. Service Provider servicing ECGC should comply with ECGC's Information Security policies in key concern areas relevant to the activity, the broad areas are:

    i. Responsibilities for data and application privacy and confidentiality.

ii. Responsibilities on system and software access controls and administration.

iii. Custodial responsibilities for data, software, hardware and other assets of Company being managed by or assigned to Service Provider.

iv. Physical security of the Services / Equipment provided by the Service Provider.

e. Service Provider shall also be required to comply with statutory and regulatory requirements as imposed by various statutes, labour laws, local body rules, State and Central Government Body statutes, and any other regulatory requirements applicable on the Service Provider, and shall produce the same for records of ECGC Limited and / or its Auditors and / or its regulator.

11. Warranty & Warranty Disclaimer

The Service Provider hereby warrants that the Service Provider shall provide the Services in accordance with **Scope of Work** and that in the course thereof, it shall exercise the same degree of professional competence, care, skill, diligence and prudence as is normally exercised by professionals in the Service Provider's field.

12. Term and Termination

(a) The term of this Agreement shall be for a period of 6 months ("**Term**"), commencing from the Effective Date. During the term of this Agreement, either party shall have the right to terminate this Agreement by giving to the other 7 days' notice in advance in writing and without assigning any reason whatsoever.

(b) In case of a breach (material in nature) under the Contract or any other subsequent documents containing obligations under the contract, the Company shall notify in writing to the Service Provider and give a period of further maximum 7 days to rectify the breach as to the Company's satisfaction. In case the breach is not rectified to the Company's satisfaction, the Company may terminate the contract.

(c) Upon termination of this Agreement before completion of the Term of this agreement, the Service Provider shall be entitled to payment of fees for the

portion of the services delivered till the last date of termination, subject to any applicable deductions with respect to penalties, damages etc.

(d) Either party may terminate the Agreement at any time and for any reason by providing seven (07) days written notice to the other party. However, both the parties shall continue performing their respective liabilities and obligations during the notice period.

(e) ECGC shall not be obligated to pay the vendor for any such terminated services performed or expenses incurred after the effective date of such termination for /without cause.

13. Working on ECGC's Holiday

Working on Saturday, Sunday, or public holidays at ECGC premises shall be only with prior permission from ECGC. Request for such permission if required, should be submitted 3 working days prior to the date of holiday, to respective location head. The Service Provider should provide the visiting Team member's details in advance to respective offices. The Team Member shall visit at the scheduled date and time and show his identity card/ permission letter when asked for.

14. Governing Laws and Dispute Resolution: This agreement shall be governed by and construed in accordance with the laws of India. The courts at Mumbai shall alone have exclusive jurisdiction for the purposes of adjudication of any dispute or differences whatsoever arising in respect of or relating to the RFP, the subsequent contract awarded or the terms and conditions of the Contract.

15. Force Majeure:

Notwithstanding the provisions of this Agreement, the Service Provider shall not be liable for any penalty, damages, or termination for default, if and to the extent, that, the delay in performance, or other failure to perform its obligations under the Contract, is the result of an event of Force Majeure.

For purposes of this clause, "Force Majeure" means an event beyond the control of the Service Provider and not involving the Service Provider's fault or negligence and not foreseeable. Such events may include, but are not restricted

to, acts of ECGC in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.

If a Force Majeure situation arises, the Service Provider shall promptly notify ECGC in writing of such condition and the cause thereof. Unless otherwise directed by ECGC in writing, the Service Provider shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

16. Miscellaneous Provisions

a. It is expressly agreed between the parties that the Contract, The Request for Proposal (RFP) Document, any addendum or corrigendum issued thereafter and the complete Annexures thereto constitute the Entire Agreement between the Parties.
b. All notices, requests, demands or other communications which are required to be given pursuant to the terms of this Agreement shall be in writing addressed to the above mentioned addresses and will be deemed to have been duly given when received. The notices shall be sent to the addresses as set forth above and to the attention of the signatories of this Agreement, or to such other addresses or individual(s) as the Parties may mutually agree in writing from time to time.
c. Service Provider agrees and undertakes that they have not directly or through any other person or firm offered, promised or given nor shall offer, promise or give, to any employee of ECGC involved in the processing and/or approval of our proposal/offer/bid/Proposal/contract or to any third person any material or any other benefit which he/she is not legally entitled to, in order to obtain in exchange advantage of any kind whatsoever, before or during or after the processing and/or approval of our proposal/offer/bid/Proposal/contract.
d. During the term of this agreement and one year thereafter, the parties shall not solicit, encourage or attempt to solicit, induce or encourage, either directly or indirectly, any of the party's personnel or employee for employment, unless prior written permission is obtained from the other party; provided however, that the foregoing shall not apply to the hiring of employees who respond to Internet

or other advertisements of general circulation not specifically targeted to such employees.

e. The relationship between Company and Service Provider is solely that of an Independent Contractor and the relationship is on a principal-to-principal basis. Nothing in this Agreement, and no course of dealing between the parties, shall be construed to create an employment or agency relationship or a partnership between a party and the other party or the other party's employees or Clients or agents
f. This Agreement shall not be assigned by either party without the prior written consent of the other party.
g. If any provision of this Agreement is held to be invalid, illegal or unenforceable, such provision will be struck from the Agreement and the remaining provisions of this Agreement shall remain in full force and effect.
h. No failure on the part of any party to exercise or delay in exercising any right hereunder will be deemed a waiver thereof, nor will any single or partial exercise preclude any further or other exercise of such or any other right.
i. Termination or cancellation of this Agreement for any reason shall not release either party from any liabilities or obligations set forth in or arising from this Agreement which remain to be performed or by their nature would be intended to be applicable following any such termination or cancellation.
j. This Agreement along with the said RFP, bid response and other annexures constitute the entire agreement between parties relating to the subject matter hereof and supersede any prior proposals, understandings, correspondence or other documents exchanged between the parties prior hereto. This Agreement can be modified, supplemented or amended only by a written agreement executed by both parties.
k. This Agreement may be executed in counterparts, which together will constitute one instrument.

IN WITNESS WHEREOF, the Parties hereto have set and subscribed their respective hands unto this Agreement on the day and date first set out hereinabove.

For and on behalf of	**For and on behalf of**
ECGC Ltd.	**SERVICE PROVIDER**
the "Company" aforesaid,	**the "Service Provider" aforesaid,**
through its authorised signatory	**through its authorised signatory**
_____	_____
NAME :	**NAME:**
DESIGNATION : GM(RMD)	**DESIGNATION:**

WITNESSES:

1. 2.

Annexure – 10: Details of Professional staff

Details of Professional staff who will be engaged for the project

(Separate Sheet for every Staff member that is likely to be involved in the project)

1. Name of Employee
2. E-mail Id
3. Phone No. (Office)
4. Mobile No
5. Date since working in the Company/Firm
6. Professional Qualifications
7. Experience

Sr. No.	Details of similar work undertaken	Brief Details of services undertaken in India/abroad and the Organization where assignment was undertaken	Period: From-To
01			
02			
03			
04			

Annexure – 11

INTEGRITY PACT

Between ECGC Limited hereinafter referred to as "The Principal", and ……hereinafter referred to as "The Bidder/ Contactor"

PREAMBLE

The Principal intends for to award, under laid down organizational procedures, contract/s for ……..(work)

The principal is a Government Company formed under the Companies Act, 1956, performing its functions as an Insurer. The Principal values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness/ transparency in its relations with its Bidder(s) and/ or Contractor(s).

In order to achieve these goals, the Principal will enter into this pre-contract Agreement, with every Contractor/Sub – Contractor/Vendor/Agency/Supplier/Bidder with whom the Principal intends to enter into any contract above the threshold value of Rs. 5,00,000/- (Rupees Five Lakhs only), falling under the scope of the 'ECGC Procurement Guidelines' as amended from time to time and administrative instructions issued thereon.

The Principal will appoint Independent External Monitor (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Provided that nothing mentioned herein shall apply to contracts of insurance, reinsurance, retrocession entered into as part of the Reinsurance business of the Principal or to agency and other service contracts in relation to the core activities of reinsurance and investment of the Principal.

Provided further that nothing mentioned herein shall apply to any branch, representative, or other offices of the Principal within India or outside India.

Section 1 - Commitments of the Principal

(1) The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

a. No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Principal will exclude from the process all known prejudiced persons.

(2) If the Principal obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Principal will inform the Chief Vigilance Officer (CVO) and in addition can initiate disciplinary actions.

Section 2 - Commitments of the Bidder(s)/ Contractor(s) which term shall include Vendor(s)/Agency(ies)/Sub-contractor (s) if any, etc.

(1) The Bidder(s)/ Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

i. The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

ii. The Bidder(s)/ Contractor (s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

iii. The Bidder(s)/ Contractor(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and information contained or transmitted electronically.

iv. The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of Agents/representatives in India, if any. Similarly, the Bidder(s)/Contractor(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further details as mentioned in the "Guidelines on Indian the Agents of Foreign Suppliers" shall be disclosed by Bidder(s)/ Contractor(s). Further, as mentioned in the Guidelines all the Payments made to the Indian agent/ representative have to be in Indian Rupees only.

v. The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents or any other intermediaries in connection with the award of the contract.

(2) The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3- Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or in any other form such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/Contractor(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 - Compensation for Damages

(1) If the Principal has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

(2) If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) The Bidder declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 - Equal treatment of all Bidders / Contractors / Subcontractors

(1) The Bidder(s)/ Contractor(s) undertake(s) to demand from his subcontractors a commitment in conformity with this Integrity Pact.

(2) The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Principal will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 - Criminal charges against violating Bidder(s) / Contractor(s) / Subcontractor(s)

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor/ Monitors

1.The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

2. One (1) IEM has been appointed by the Central Vigilance Commission (CVC). Details of IEM are as follows: a) Shri Uppuluri Krishna Murty, ukmirts86@gmail.com , Door No 31-51-5/84, Greencity, Near Apparels Export Promotion Park, Vadlapudi Gajuwaka Mandal, SRO - Gajuwaka, Post Office: Special Economic Zone, District: Visakhapatnam, Andhra Pradesh - 530046 (Mob. No. 7045592460 & 7045592461, E-mail: ukmirts86@gmail.com).

3. The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Chairman, ECGC Ltd.

4. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Principal including that

provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidder(s)/ Contractor (s)/ Subcontractor(s) with confidentiality.

5. The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

6. As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Principal and request the Management to discontinue or take corrective action, or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

7. The Monitor will submit a written report to the Chairman cum Managing Director (CMD) of ECGC Ltd. within 8 to 10 weeks from the date of reference or intimation to him by the Principal and, should the occasion arise, submit proposals for correcting problematic situations.

8. If the Monitor has reported to the CMD, ECGC Ltd., a substantiated suspicion of an offence under relevant IPC/ PC Act, and the CMD, ECGC Ltd. has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

9. The word 'Monitor' would include both singular and plural.

Section 9 - Pact Duration

This Pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. If any claim is made / lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged / determined by CMD of ECGC Ltd.

Section 10 - Other provisions

1.This agreement is subject to Indian Law. Place of performance and jurisdiction is the Head Office of the Principal, i.e., Mumbai.

2. Changes and supplements as well as termination notices need to be made in writing.
3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.
4. Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. In the event of any contradiction between the Integrity Pact and its Annexure, the Clause in the Integrity Pact will prevail.

_____ _____

(For & On behalf of the Principal) (For &On behalf of Bidder/Contractor)

(Office Seal)

Place ---------- (Office Seal)

Date ----------

Witness 1:

(Name & Address) _____

_____

_____

Witness 2:

(Name & Address) _____

_____

_____

Annexure – 12: Bank Guarantee for Performance Guarantee

(On non-judicial stamp paper of value Rs.500/-)

To,
ECGC Limited
ECGC Bhawan, CTS No. 393, 393/1-45, M.V. Road, Andheri (East),
Mumbai – 400069

BG No_____ Date_____
Amount of Guarantee: Rs. _____
Guarantee cover from ___ to _____
Last Date for Lodgment of Claim:

IN CONSIDERATION OF ECGC LIMITED, a company incorporated under the Companies Act 1956 and having its registered office at ECGC Bhawan, CTS No. 393,393/1-45, M.V. Road, Andheri (East), Mumbai – 400069
(hereinafter referred to as the "the Purchaser" which expression shall, unless it be repugnant or contrary to the subject or context thereof, be deemed to mean and include its successors and assigns) having awarded to _____a company registered under the _____ having its Registered office at _____ (hereinafter called the Vendor which expression shall, unless it be repugnant or contrary to the subject or context thereof, be deemed to mean and include its successors and assigns) a contract by issue of work order vide Order No. _____
(hereinafter called "the order" which expression shall include any amendments/alterations to "the order" issued by "the Purchaser") and the same having been unequivocally accepted by the vendor resulting in a contract bearing No. _____ dated _____ value at _____ for SELECTION OF SERVICE PROVIDER FOR CONDUCTING CYBER SECURITY POSTURE ASSESSMENT as stated in the said Order and the Vendor having agreed to provide a contract performance guarantee equivalent to _____ % of the said value for the faithful discharge of vendor's entire obligations and liabilities in connection with the said order

1. We, …….. ….. …. Bank (name and address) having registered office at ..... (hereinafter referred to as "the Bank" which expression shall include its successors and assigns) hereby guarantee and undertake to pay to the

Purchaser without any demur, reservation, contest, recourse, or protest on first demand an amount

not _____(amount in figures and words) being ___% of the order value against any loss or damage, costs, charges and expenses caused to or suffered by the Purchaser by reason of non-performance and non-fulfilment or for any breach on the part of the Vendor of any of the terms and conditions of the said order.

2. The Bank further agree that the Purchaser shall be sole judge whether the said Vendor has failed to perform or fulfil the said order in terms thereof or committed breach of any terms and conditions of the order and the extent of loss, damage, cost, charges and expenses suffered or incurred or would be suffered or incurred by the Purchaser on account thereof and we waive in the favour of the Purchaser all the rights and defenses to which we as guarantors may be entitled to.

3. The Bank further agrees that the amount demanded by the Purchaser as such shall be final and binding on the Bank as to the Bank's liability to pay and the amount demanded notwithstanding any dispute or difference between the Purchaser and the vendor or any suit or other legal proceedings including arbitration pending before any court, tribunal or arbitrator relating thereto, our liability under this guarantee being absolute and unconditional.

4. The Bank further agrees that the Purchaser shall have the fullest liberty, without our consent and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said order or to extend time of performance by the Vendor from time to time or to postpone the time for enforcement of any of the powers exercisable by the Purchaser against the Vendor and to forbear to enforce any of the terms and conditions relating to the order and we shall not be relieved from our liability by reason of any such variation or extension being granted to the Vendor or for any forbearance, act or omission on the part of the Purchaser or any indulgence by the Purchaser to the Vendor or by any such matter or things whatsoever which under the law relating to sureties would have the effect of relieving us.

5. The Bank undertakes not to revoke this guarantee during its currency (till last date for claim lodgment) except with the previous consent of the Purchaser in writing and further agrees that the guarantee herein contained shall continue to be enforceable till the Purchaser discharges this guarantee.

6. The Bank also agree that the Bank's liability under this guarantee shall not be affected by any change in the constitution of the Vendor or dissolution ……

7. The Bank also agrees that the purchaser at its option shall be entitled to enforce this guarantee, against the Bank as principal debtor, in the first instance without proceeding against the vendor and not withstanding any security or other guarantees that the Purchaser may have in relation to the Vendor's liabilities.

8. Notwithstanding anything contained herein above:

i. The Bank's liability under this guarantee shall not exceed Rs.

ii. This Bank Guarantee shall be valid up to and including _____ unless extended on demand by the Vendor on whose behalf this guarantee has been given and the Purchaser shall have the right to demand or claim or encash/negotiate this Bank guarantee within 8 weeks after the aforesaid date i.e. _____

iii. The Bank is liable to pay the guarantee amount or any part thereof under this Bank Guarantee only and only if the Purchaser serves upon the Bank a written claim or demand on or before _____ (validity + 8 weeks from the date of expiry of this guarantee).

9. This Guarantee shall be governed by Indian laws and the Courts at Mumbai, India shall have the exclusive jurisdiction.

IN WITNESS WHEREOF the Bank has executed this document on this..... day of .....

For ..... Bank

(by its constituted attorney)

(Signature of a person authorized to sign on behalf of "the Bank")

Witness:

1. Name: ……

Designation:

Address:

2. Name: ……..

Designation:

Address:

NOTE:-

1. Indigenous Vendor or Foreign Vendor through Indian Bank to submit BG.

2. Please forward original Bank Guarantee along with Banker Authenticity Letter directly through Bank. If BG is not received directly from Bank then ECGC Ltd. shall get the Bank Guarantee verified and only on confirmation of verification the Bank Guarantee shall be considered as submitted. Expenses for BG verification shall be borne by ECGC Ltd.