(A Government of India Enterprise)

You focus on exports. We cover the risks.

REQUEST FOR TENDER
(LIMITED TENDER ENQUIRY)

FOR
ANNUAL CYBERSECURITY & SYSTEMS AUDIT

Ref: ECGC/Tender-06/RMD/11/2021-22

Date: 21-01-2022

ECGC LIMITED

10th Floor, Express Tower, Nariman Point, Mumbai - 400021

Contents

Section 1 ..... **4**

1. Introduction 4

1.1. Invitation to Bidders 4

1.2. Schedule of events 5

Section - 2 ..... **6**

2. Disclaimer 6

Section - 3 ..... **7**

3. Instructions for Bidder(s) 7

3.1. General Instructions 7

3.2. Scope of Work & Deliverables Timeline 9

3.3. Rights of ECGC: 9

i. ECGC does not bind itself to accept the lowest quotation and reserves the right to reject any or all the quotations received, without assigning any reason thereof. 9

ii. While processing the Bids, ECGC further reserves the right to delete or reduce any item or section contained in the Tender Document or in the Scope of Work without assigning any reason thereof. 9

3.4. Professional Staffs 9

3.5. Queries: 10

3.6. Bidding process 10

3.7. Period of Validity of Bids 11

3.8. Opening and evaluation of bids 11

Section – 4 ..... **13**

Award of Contract 13

Section - 5 ..... **14**

5. TERMS AND CONDITIONS OF CONTRACT (TCC) 14

Section – 6 ..... **15**

Annexure – 1: Scope of Work & Deliverables Timeline 15

List of Abbreviations used in the Scope of Work 23

Annexure – 2: Details of Professional staff 24

Annexure – 3: Queries Format 25

Annexure – 4 : Price / Commercial Bid Format 26

Annexure – 5: Acknowledgement 28

Annexure – 6: Format for Letter of Authorization 30

Annexure – 7 : Service Agreement 31

Scope of Work & Deliverables Timeline.....46
List of Abbreviations used in the Scope of Work 55
Annexure – 8 : Bank Details 56

Section 1

1. Introduction

1.1. Invitation to Bidders

By way of this Request for Tender (‘**RFT’**) Document, (hereinafter also referred to as ‘the Bid Document’ or ‘the Tender Document’) **ECGC Limited** (hereinafter referred to as ‘ECGC’), a company wholly owned by Government of India and set up in 1957, invites competitive Bids from the CERT-In Empaneled Information Security Auditing Organizations from Mumbai (hereinafter referred to as (‘**the Bidder(s)**’.) for **“Cybersecurity Audit” as per scope of work defined in Annexure – I of this RFT.**

The “Price/Commercial Bids” along with other documents would be received in physical form.

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

Please note that all the required information as sought in the Tender Document shall be provided by the bidders. Incomplete information may lead to rejection of the Bid. The Company reserves the right to change the dates mentioned in this RFT Document, which will be communicated to the Bidder(s), and shall be displayed on ECGC’s website. The information provided by the Bidder(s) in response to this RFT Document will become the property of ECGC and will not be returned. ECGC reserves the right to amend, rescind or reissue this RFT Document and all subsequent amendments, if any to this RFT Document. Amendments or changes shall be communicated directly and/or displayed at ECGC’s website only.

1.2. Schedule of events

RFT Document Availability	The RFT Document will be shared through e-mail to selective CERT-In empaneled auditors from Mumbai and published on the website of ECGC.
Last date of submission of Bids	04/02/2022
Pre-bid Queries (if any)	21-01-2022 to 03-02-2022
Opening of Price/Commercial Bids	08/02/2022
Contact Details: Chief Information Security Officer (CISO): 022-66590620/+91-8080138143 Executive Officer (RMD) : 022 -66590581	
Address for Communication and submission of Bid.	CISO ECGC Limited, Express Towers, 10th Floor, Nariman Point, Mumbai – 400 021
Telephone	022-66590620
All correspondence / queries relating to this RFT Document should be sent to / through following email ID only	security@ecgc.in

NOTE: Timelines are subject to change at the sole discretion of ECGC Ltd.

Section - 2

2. Disclaimer

The information contained in this RFT 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 RFT document and all other terms and conditions subject to which such information is provided.

This RFT Document is neither an agreement nor an offer and is only an invitation by ECGC to the interested parties for submission of Bids. The purpose of this RFT Document is to provide the Bidder(s) with information to assist the formulation of their bids.

This RFT Document does not claim to contain all the information each Bidder may require. ECGC shall incur no liability under any law, statute, rules or regulations as to accuracy, reliability or completeness of this document. ECGC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFT Document.

ECGC reserves the right to reject any or all the bids received in response to this document at any stage without assigning any reason 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 document will become the property of ECGC and will not be returned. No contractual obligation whatsoever shall arise from the RFT process until a formal contract is signed and executed by duly authorized representatives of ECGC with the selected Bidder.

Section - 3

3. Instructions for Bidder(s)

3.1. General Instructions

3.1.1 Before bidding, the Bidder(s) are requested to visit the ECGC website https://www.ecgc.in and also carefully examine the Tender Document and the General Terms and Conditions of the Contract (TCC) contained therein, and if there appears to be any ambiguity or discrepancy between any terms of the Tender Document and the Contract, they should immediately refer the matter to ECGC for clarifications.

3.1.2 The Bidder, for the purpose of making the Bid, shall complete in all respects, the form(s) annexed to the Tender Document, quote the prices and furnish the information/ documents, called for therein, and shall sign and put date on each of the forms/documents in the space provided therein for the purpose. The Bidder shall affix its initial on each page of the Bidding Documents.

3.1.3 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. In case of a consortium, the Bid shall be signed by the officer (s) so authorized by each consortium member and the Bid shall be affixed with the common seals of each member of the consortium.

3.1.4 The Bid shall contain the address, Tel. No., Fax No. and e-mail id, if any of the Bidder, for the purposes of serving notices required to be given to the Bidder in connection with the Bid.

3.1.5 The Bid form and the documents attached to it shall not be detached from one another and no alteration or mutilation (other than filling in all the blank spaces) shall be made in any of the forms or documents attached thereto. Any alterations or changes to the entries in the attached documents shall only be made by a separate covering letter otherwise it shall not be entertained for the Bidding process.

3.1.6 The Bidder, irrespective of its participation in the bidding process, shall treat the details of the documents as privileged, secret and confidential.

3.1.7 ECGC does not bind itself to accept the lowest of any Bid or any other bid received and shall has the right to reject any Bid without assigning any reason whatsoever. ECGC also reserves the right to re-issue the Tender Document.

3.1.8 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 decision of ECGC shall be final and binding on the Bidder. The Bidder should ensure that ambiguous or unquantifiable costs/ amounts are not included in the Bid, which would disqualify the Bid.

3.1.9 Each Bidder can submit only one Bid.

3.1.10 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.

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

3.1.12 All rates and total amount should be written both in figures and in words and if there is any discrepancy between the two, the lowest amount will only be accepted.

3.1.13 No questions or items in the annexures shall be left blank or unanswered. Where you have no details or answers to be provided a 'No' or 'Nil' or 'Not Applicable' statement shall be made as appropriate. Forms with blank columns or unsigned forms will be summarily rejected.

3.1.14 Bids not confirming to the requirement of the RFT may not be considered by ECGC. However, ECGC reserves the right at any time to waive any of the requirements of the RFT.

3.1.15 Bids must be received by ECGC at the address specified, no later than the date & time specified in the "Schedule of Events" in Invitation to Bid.

3.1.16 ECGC is not responsible for non-receipt of bids within the specified date due to any reason including postal delays or holidays.

3.1.17 Any Bid received after the deadline for submission of Bids prescribed, will be rejected and subsequently destroyed. No Bids shall be returned.

3.1.18 ECGC may, at its discretion, extend the deadline for submission of Bids by amending the appropriate terms and conditions in the Bid Document, in which case, all rights and obligations of ECGC and Bidders previously subject to the deadline will thereafter be subject to the extended deadline, which would also be advised to all the interested Bidders on ECGC's website.

3.1.19 ECGC reserves the right to accept or reject any Bid or to cancel the Bidding process and reject all Bids at any time prior to contract award, without incurring

any liability to the affected Bidder or Bidder(s). All decisions taken by ECGC are binding and final.

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

3.1.21 The bid is liable to be disqualified in the following cases:

i. Bid not submitted in accordance with RFT;

ii. Bid received in incomplete format;

iii. Bid is not accompanied by all requisite documents;

iv. Bid is received after the due date;

v. an unsolicited bid.

3.1.22 The bids once submitted cannot be modified or altered.

3.1.23 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.

3.2. Scope of Work & Deliverables Timeline

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

3.3. Rights of ECGC:

i. ECGC does not bind itself to accept the lowest quotation and reserves the right to reject any or all the quotations received, without assigning any reason thereof.

ii. While processing the Bids, ECGC further reserves the right to delete or reduce any item or section contained in the Tender Document or in the Scope of Work without assigning any reason thereof.

3.4. Professional Staffs

The selected bidder shall provide to ECGC a list of Professional Staffs along with their respective CVs mentioning their relevant experience as per Annexure 2. The said list along with the CVs shall be evaluated by ECGC and only those professional staffs shall work on the project as approved by ECGC.

3.5. Queries:

The Bidder(s) having any doubt/ queries/ concerns with any clause of this document or selection process shall raise their concern within 7 days of release of RFT Document in the format annexed at Annexure – 3. ECGC will not be liable to accept or provide any explanation towards any doubt/ concerns beyond the deadline of 7 days from the release of RFT document.

All the queries shall be communicated only through the e-mail id provided, security@ecgc.in the format provided in Annexure - 3.

ECGC would issue clarifications/ amendments in writing via e-mail/website and the same will become part of RFT.

3.6. Bidding process

3.5.1 The interested bidders should submit their proposal in a sealed NON-WINDOW envelope superscripted with "Quotation for Cybersecurity Audit" form or via e-mail to security@ecgc.in before the last date of submission of bids.

3.5.2 The Bid shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. The envelope shall be addressed to ECGC at the said address given in Section 1.2; and

a) Bear the Project Name

b) The envelops shall contain completely filled documents in the following order:

(i) Annexure – 2: Details of Professional Staff;

(ii) Annexure – 4: Commercial Bid;

Note: If sending via e-mail then it is mandatory for the price proposal to be a password protected document on the letter head of the bidding company

(iii) Annexure – 5: Acknowledgment;

(iv) Annexure – 8: Bank Details.

3.5.3 All envelopes should indicate the name and address of the Bidder on the cover.

3.5.4 If the envelope is not sealed and marked, ECGC will assume no responsibility for the Bid's misplacement or its premature opening.

3.5.5 Prices are to be quoted in Indian Rupees only in the format at Annexure - 4.

3.5.6 Prices quoted should be exclusive of all Central / State Government levies, taxes (including Service Tax / GST).

3.5.7 Prices quoted by the Bidder shall be fixed during the Bidder's performance of the Contract and shall not be subject to variation on any account, including exchange rate fluctuations, during the validity period of the contract. Taxes / Duties / Levies / Cess etc. levied by Central or State Governments, or Statutory, Quasi-Government Bodies, or Regulators may be charged as per actuals, and are allowed to be varied. A Bid submitted with an adjustable price quotation, other than exceptions specified herein, will be treated as non-responsive and shall be rejected.

3.7. Period of Validity of Bids

3.5.8 Bids shall remain valid for a period of 60 days from the date of opening of the Bid. The fees quoted shall remain fixed during the currency of the Contract unless agreed otherwise by ECGC. Bidder shall not be entitled during this period to revoke or vary the content of Bid or any term thereof. In such case of making any variation subsequent to submission of bid, the offer shall be treated as "REJECTED".

3.5.9 In exceptional circumstances, ECGC 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 RFTs or any debarment.

3.5.10 The Company reserves the right to call for fresh quotes any time during the validity period of the Bid, if considered necessary.

3.8. Opening and evaluation of bids

3.7.1. Opening of Bids by ECGC

3.7.1.1 ECGC reserves the right to open the Bids soon after their receipt from all the Bidder(s) without waiting till the last date as specified above and also the right to disqualify any or all Bidder(s) either on the basis of their responses, to all or some of the response sheets, or even any part thereof without assigning any reasons whatsoever.

3.7.1.2 ECGC will examine the Bids to determine whether they are complete, whether the required formats have been furnished, the documents have been properly signed, and that the Bids are generally in order.

3.7.1.3 Prior to the detailed evaluation, ECGC will determine the responsiveness of each Bid to the Bid Document. For purposes of these clauses, a responsive Bid is one, which conforms to all the terms and conditions of the Bid Document without any deviations.

3.7.1.4 Only those Bidders and Bids which have been found to be in conformity of the terms and conditions of RFT during the preliminary evaluation would be taken up by ECGC for further detailed evaluation.

3.7.1.5 Bidder(s) bidding in the process shall give as a part of the Bidding documents a statement on their letter head, as per the format provided under Annexure - 5, that they have no objection with any clause of the Tender Document.

3.7.1.6 No Bidder shall contact ECGC on any matter relating to its Bid, from the time of opening of Price/Commercial Bid to the time the Contract is awarded.

3.7.1.7 Any effort by a Bidder to influence ECGC in its decisions on Bid evaluation, Bid comparison or contract award may result in the rejection of the Bidder's Bid and barring from any future RFTs / contracts / business with ECGC.

3.7.1.8 A maximum of two persons from each bidder can attend the bid opening. The bidders have to authorize two persons in format provided at Annexure – 6 and inform ECGC in advance or attend via web-conferencing link as facilitated by ECGC Ltd.

Section – 4

Award of Contract

The Bidder that bids the lowest commercial bid shall be awarded the Contract. However, ECGC shall be under no obligation to accept the lowest or any bid received and shall be entitled to reject any or all bids without assigning any reason whatsoever. ECGC Ltd. will notify the successful Bidder in writing, by letter or by e-mail, that its Bid has been accepted. The notification of award will constitute the formation of the offer to contract. The selected Bidder should convey acceptance of the award of contract by returning duly signed and stamped duplicate copy of the award letter within seven working days of receipt of the communication. In case of a tie, the Bidder that conducted similar type of systems audit and cyber security testing in other Government undertakings/enterprises will be given preference. In case the selected Bidder fails to accept the award then the Bidder having the next lowest commercial bid among the Bidder(s) (other than the Bidder who has failed to accept the award) will be considered for the award and so on. The successful Bidder will have to execute a Service agreement within 15 working days of the award of Contract, which will be valid for the tenure as mentioned in this RFT Document. The draft of the same is annexed herein below as Annexure – 7. ECGC reserves the right to alter / vary / amend / modify all or any of the terms set out in the said draft Agreement before the same is signed.

Section - 5

5. TERMS AND CONDITIONS OF CONTRACT (TCC)

As stated in draft Service Agreement at Annexure 7.

Section – 6

Annexure – 1: Scope of Work & Deliverables Timeline

Background

ECGC intends to undertake a review of its adherence to the regulatory requirements of Insurance Regulatory and Development Authority of India (IRDAI) pertaining to Cyber Security.

Current State of Information Technology (herein after referred as IT) In ECGC

ECGC has the following IT applications in operation:

1. An Enterprise Resource Planning (ERP) System, supporting all Core Insurance and non-core functions of ECGC, including Enterprise Accounting and MIS.
2. A Public Portal, catering to the general public, offering information on ECGC's products and services, public disclosures, and company information.
3. A Client Portal, catering to Exporter and Banker clients.
4. A Grievance Management Portal, IGMS, as mandated by the regulator IRDAI, to manage customer complaints.
5. A Treasury software system, supporting the Treasury operations of ECGC.
6. A RBI-NDS system for supporting the Treasury operations of ECGC.
7. An Enterprise Email solution for all employees.
8. A web content filtering solution for employee browsing needs and to filter against malware.
9. A messaging security solution to filter malware and spam in emails.
10. An Antivirus solution for all servers and employee PCs.
11. A patch management solution for servers and employee PCs.
12. An Active Directory solution for single sign on (partial) and managing group policies.
13. A biometric system for managing employee attendance / reimbursements.
14. A swipe card system for some employees for access control to some office.
15. A Hypervisor solution for managing virtualization.

The above applications are supported by a SAN-based storage solution, multiple switches, and firewalls (virtualized). ECGC employees are connected to the various applications via a MPLS VPN and freshly rolled out SD-WAN. All major systems /

services used by employees are centralized. The management of the IT setup (DC & DRC) is outsourced to a third-party.

Purpose of Audit

ECGC envisages a review of its processes and IT infrastructure with respect to the following areas:

1. Review based on IRDAI Circular Ref No: IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 (Guidelines on Information and Cyber Security for Insurers) and amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020
2. ITGC (General Controls) Audit for IT systems handling Financial Information
3. Vulnerability Assessment and Penetration Testing of IT Systems

The auditor shall also assist ECGC Ltd. in the following areas pertaining to the IRDAI Circulars -

1. Adhering to changed or updated timelines of compliance
2. Adhering to further clarifications issued by IRDAI
3. Providing additional certification/s and clarifications as required by the IRDAI from the cyber security auditor

The audit will include but not limited to the testing of Applications, review of Information Security Policy & Procedures, Gap Assessment in IT security and Procedures, Assessment of Network Security & Information Security solutions, Vulnerability and Penetration testing, review of Data Centre including physical visits, compliance with IRDAI, and submission of reports. The backbone IT infrastructure of the Company is located at Mumbai and Data Centre at Faridabad.

Based on the approach mechanism and intended outcome the scope of work is outlined into two parts-

Part A: Systems and Process Audits and
Part B: Technical Cybersecurity VAPT Audit

The bidder has to undertake the following process audits with respect to Technology Governance, Risk and Compliance under Part A

A.1. Cybersecurity Audit

A.2. IT Systems Audit

Following are key indicative but not exhaustive scope of work to be carried out by the selected Bidder -

A.1. Cybersecurity Audit

Review based on IRDAI Circular (Guidelines on Information and Cyber Security for Insurers) Ref No. IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 and amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020

IRDAI's information and cyber security guidelines and Annexure A (control checklist) covering all of the below areas but not limiting to -

1. Enterprise Security
2. Information Asset Management
3. System acquisition, development and maintenance
4. Information Security Risk Management
5. Data & Communication Security
6. Application, Mobile & Cloud Security
7. Cyber Security
8. Platform / Infrastructure Security
9. Network & Endpoint Security
10. Cryptography & Key Management
11. Security Logging & Monitoring
12. Virtualization
13. Information System Audit
14. Organization of information security
15. Human resource security
16. Access Control
17. Cryptography
18. Physical Access and Environmental controls
19. Operations security
20. Communication Security
21. Information security in supplier relationships
22. Information security incident management

23. Compliance with legal requirements
24. Business Continuity Management
25. Compliance
26. Cloud Security
27. Information and Cyber Security Policy
28. Cyber Security Assurance Programme

A.2. IT Systems Audit

Perform a review of the areas pertaining to IT General Controls and System readiness. The bidder shall incorporate this audit activity in parallel to above process audit and submit a separate Report on the same.

The areas are as mentioned below, however they are not limiting to -

1. Change Management
2. IT Governance
3. IT Strategy
4. Security Policy, Procedures and Frameworks
5. Incident & Problem Management
6. Backup Management
7. Access Management
8. Patch Management
9. Physical & Environmental Control
10. IT security risk assessments
11. Functionality review
12. IT landscape review
13. Review of IT operations
14. Review of information security
15. Review of third-party suppliers and outsourcing
16. Review of design of Business Continuity (BC) and Disaster Recovery (DR)
17. Review of IT operations
18. Conduct walkthroughs and reviews of identified in-scope controls pertaining to the review areas in scope
19. Conduct meetings with relevant stakeholders to understand the process of capacity planning for applications and IT infrastructure
20. Obtain and review relevant evidences for each control

21. Perform sample-based testing where relevant
22. Identify and document control gaps
23. Discuss identified gaps with stakeholders
24. Present reports for each of the above areas
25. Discuss and finalize the risk register with the IT Security function head - CISO
26. Suggest implementation guidelines based on the industry best standards & a prioritized roadmap to achieve the recommendations of the review report.

Key Stages of A.1 and A.2 Process based Audits:

1. Kick-off Meeting & Stakeholder Identification
2. Audit Preparation on site & Related documentation to be shared
3. Audit Process
4. Prepare list of pre-requisites with respect to the above areas and share the same.
5. Conduct walkthroughs and reviews of identified in-scope controls pertaining to the review areas in scope
6. Obtain and review relevant evidences for each control
7. Perform sample-based testing where relevant
8. Present reports for each of the above areas
9. Identify and document control gaps
10. Discuss identified gaps with stakeholders
11. Provide GAP analysis report and recommendations to address the identified the gaps.
12. Suggest implementation guidelines based on the industry best standards & a prioritized roadmap to achieve the recommendations of the review report.
13. Create roadmap for addressing identified gaps with prioritization
14. Create roadmap and strategy to address all identified shortcomings.
15. Prioritize the solution w.r.t. organization’s posture (Immediate measures/long term measures)
16. Recommend the best fit solutions & controls
17. In collaboration with ECGC IT staff, resolve all the gaps identified in the gap analysis, vulnerabilities found, additional vulnerabilities pointed out by ECGC and make ECGC ready for final audit.
18. Perform the final Audit in lines to above scope
19. Draft Audit Report Generation & Discussion

20. Final Audit Report Submission, Discussion (Two separate Audit reports signed by CISA Auditor shall be submitted for A.1 & A.2 respectively)
21. Finalize the prioritized implementation roadmap
22. Re-assessment of Cyber Maturity Rating Scale and Final Ratings post the Audits

Part B: Technical Cybersecurity VAPT Audit

The bidder shall conduct technical testing on the IT Systems, OS, Applications and Network and report the vulnerabilities.

The scope of this Vulnerability Assessment – Penetration Testing Audit report is as below –

1. Internal Network Vulnerability Management
    a. 65(internal IPs)
2. External Black Box Network & Application PT
    a. 4(external IPs)
3. Web Application security testing (Black Box) must also include complete proof of exploit in all cases of all the reported vulnerabilities
4. ECGC websites should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) 2021 standard
5. The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website “Certified for Security”.
6. Auditor must test website for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/application.
    i. Vulnerabilities to SQL Injections
    ii. CRLF injections
    iii. Directory Traversal
    iv. Authentication hacking/attacks
    v. Password strength on authentication pages
    vi. Scan Java Script for security vulnerabilities
    vii. File inclusion attacks
    viii. Exploitable hacking vulnerable
    ix. Web server information security
    x. Cross site scripting

xi. PHP remote scripts vulnerability
xii. HTTP Injection
xiii. Phishing a website
xiv. Buffer Overflows, Invalid inputs, insecure storage etc. Any other attack that can be a vulnerability to the website or web applications.

7. Generate all security testing reports and provide recommendations.
8. Suggest the best possible patching and remediation for the identified vulnerabilities.
9. Discuss and document the management action plan with timeline to implement the recommendations on the same
10. In collaboration with ECGC IT staff, resolve all the gaps identified in the vulnerabilities assessment and penetration testing, and re-assess the vulnerability post closure of gaps.

NOTE:

1. The complete exercise including process audit and technical VAPT testing has to be done on premise at ECGC office only.
2. The bidder has to re-assess the existing Cyber Maturity Model-Rating score and provide the final ratings for current year, post the Audit.

THE OVERALL RESPONSIBILITY OF THE SERVICE PROVIDER IS TO ENSURE ECGC'S COMPLIANCE TO ALL REGULATIONS RELATING TO GUIDELINES ON INFORMATION AND CYBER SECURITY AS ISSUED BY IRDAI.

The Selected Bidder is expected to carry out its assignment with due diligence and in accordance with prevailing standards of the profession. The selected bidder has to make a project plan to deliver all Audit Reports within timelines and present the same to the ECGC Management. The bidder shall be free to merge common areas of review and carry-out sampling processes and walkthrough discussions in a non-repetitive manner.

The selected bidder shall be accountable and responsible for the services required to be performed and it shall not be an excuse that the employee/personnel or key person of the selected bidder committed mistakes or left the bidder during the continuance of the project as per this RFT or for any other reason whatsoever.

Deliverables with Timelines

Sl. No.	Deliverables	Expected Timelines
Part A		
1.	Final Cybersecurity Audit Report	2-3 Weeks
2.	Final IT Systems Audit Report	
Part B		
4.	VAPT Security Testing Reports	1-2 Week/s

List of Abbreviations used in the Scope of Work

S.No.	Abbreviation	Full Form / Remark
1.	ERP	ENTERPRISE RESOURCE PLANNING
2.	MIS	MANAGEMENT INFORAMTION SYSTEMS
3.	IGMS	INTEGRATED GRIEVANCE MANAGEMENT SYSTEM
4.	NDS	NEGOTIATED DEALING SYSTEM
5.	SAN	STORAGE AREA NETWORK
6.	MPLS	MULTI-PROTOCOL LABEL SWITCHING
7.	VPN	VIRTUAL PRIVATE NETWORK
8.	SD-WAN	SOFTWARE DEFINED WIDE AREA NETWORK
9.	BC-DR	BUSINESS CONTINUITY – DISASTER RECOVERY
10.	ITGC	INFORMATION TECHNOLOGY GENERAL CONTROLS
11.	IRMS	INVESTMENT RISK MANAGEMENT SYSTEMS
12.	IT	INFORMATION TECHNOLOGY
13.	URL	UNIFORM RESOURCE LOCATOR
14.	IRDAI	INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA
15.	CISC	CORPORATE INFORAMTION SECURITY COMMITTEE
16.	VA	VULNERABILITY ASSESSMENT
17.	PT	PENETRATION TESTING
18.	OS	OPERATNG SYSTEM
19.	DB	DATABASE SYSTEMS

Annexure – 2: 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 – 3: Queries Format

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

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

Annexure – 4 : Price / Commercial Bid Format

PRICE/COMMERCIAL BID FOR CYBERSECURITY AUDIT

(Must be submitted in the **sealed envelope** as mentioned above)

COMPANY NAME: _____

ADDRESS:

_____

CONTACT PERSON: _____ PHONE NUMBER: _____

EMAIL: _____ WEB SITE:

_____

We submit our Price/commercial bid (fees) for the proposed assignment as under:

Sr. No.	Milestone Description	Amount in INR
Part A		
1.	Final Cybersecurity Audit Report to be submitted to CISC and IRDAI	
2.	Final IT Systems Audit Report to be submitted to CISC	
Part B		
3.	Security Testing Reports	

Terms and Conditions:

1) The above quoted fee is inclusive of all expenses excluding taxes.
2) We undertake to deliver all the deliverables as envisaged in the proposal / agreement and complete the assignment within the time frame stipulated in the RFT document.
3) ECGC Ltd will deduct tax (TDS) while releasing payment, if applicable as per the provisions of Income Tax Act, and all other applicable taxes, levies, cess etc.
4) ECGC reserves the right to negotiate and change the milestones / payment schedule / percentages with the successful bidder.

Signature of the Authorized Signatory of Company

Name:

Designation:

Contact no. (Mobile):

Email Id:

Company Seal:

Annexure – 5: Acknowledgement

Date:

To,
Chief Information Security Officer
Risk Management Division,
ECGC Limited,
Express Towers, 10th Floor,
Nariman Point,
Mumbai - 400021

Dear Sir/Madam,

Subject: Response to the Request for Tender for "CyberSecurity Audit"

1. Having examined the Request for Tender Document including Annexures, the receipt of which is hereby duly acknowledged, we, the undersigned offer to provide services in accordance with the scope of work as stated in the RFT 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 RFT.

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 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 RFT Document and all amendments any time during the tendering.

5. We agree that we have no objection with any of the clauses and bidding process of this Tender Document.

……

Signature of the authorized Signatory of Company

(Company Seal)

Name :

Designation :

Contact No (Mobile) : Email ID :

Annexure – 6: Format for Letter of Authorization
(To be submitted on the Bidder's letter head)

To,

Chief Information Security Officer

Risk Management Division,

ECGC Limited,

Express Towers, 10th Floor,

Nariman Point,

Mumbai - 400021

Letter Of Authorisation For Attending Bid Opening for Tender Ref: ECGC/Tender-04/IT/09/2019-20

The following persons are hereby authorized to attend the bid opening on _____(date) in the tender for **"REQUEST FOR TENDER FOR CYBERSECURITY AUDIT**" on behalf of M/S_____ (Name of the Bidder) in the order of preference given below:

Order of Preference Name Designation Specimen Signature

I

II

(Authorized Signatory of the Bidder)

Date_____

(Company Seal)

1. Maximum of two persons can be authorized for attending the bid opening.
2. Permission for entry to the hall where bids are opened may be refused in case authorization as prescribed above is not submitted.

Annexure – 7 : Service Agreement

This **SERVICE AGREEMENT** ("**Agreement**") is made and entered into on this the [•] day of [•] Two Thousand and Twenty [___/[___]/2022), BY AND BETWEEN:

ECGC Ltd., a Public Sector Enterprise wholly owned by Government of India, having its registered office at 10th Floor, Express Tower, Nariman Point, Mumbai – 400021 (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

SERVICE PROVIDER, a company incorporated under the Indian Companies Act, 1956, 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;

2. The Service Provider is, *inter alia*, involved in the business of providing Cybersecurity Services.

3. The Company floated Request For Tender (Limited Tender Enquiry) having reference: **ECGC/Tender-06/RMD/11/2021-22** (hereinafter referred to as "the said RFT") (Attached as Annexure – I to this Agreement).

4. The Service Provider has become the successful bidder in the said RFT and the Company has selected the Service Provider to conduct cybersecurity audit 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 whose eligibility Bid has been accepted and who was L1 as per its commercial bid 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 the agreement entered into between ECGC and the Service Provider, and signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein;

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 Annual Cybersecurity and Systems Audit.

vii. “The Project Site” means designated locations of ECGC as may be specified in Purchase Order / RFT.

viii. 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 Indian Evidence Act, 1872, 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 SERVICES

2.1. The Company hereby appoints the Service Provider to provide the 'Services' clearly set out under the '**Scope of Work** as per Annexure – I 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.

2.2. 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.

2.3. 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. FEES AND PAYMENT TERMS

3.1. Payment shall be made in Indian Rupees.

3.2. Payment shall be made via electronic fund transfer only to the bank account specified, as per the form provided under Annexure -8, in the RFT response.

3.3. No payment shall be made in advance on award of the contract.

3.4. 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, on milestone basis.

3.5. 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 other than the agreed amount as per the contract.

3.6. 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**.

3.7. 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.

3.8. All payments shall be subject to TDS and any other taxes as per the tax rules prevalent at the time of payment.

3.9. All the payments would be against the submission of the invoices to the Company along with the relevant supporting documents, if any.

3.10. 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**.

3.11. Payment Milestone:

Payment will be released according to deliverables mentioned in the table below:

S. No.	Deliverables	Payment as per Commercial Bid
1.	Final CISA signed Audit Reports Submission (for all process audits A.1 and A.2 as described in detailed Scope of Work) & Cyber Maturity Rating Scale with Final Ratings	65%
2.	Final VAPT Reports Submission (re-validation testing reports, as described in detail Scope of Work - Part B)	35%

4. SERVICE PROVIDER'S RESPONSIBILITIES

4.1. The Service Provider shall be responsible for:

4.1.1. 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.**

4.1.2. 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;

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

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

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

5. COMPANY'S RESPONSIBILITIES

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

5.1.1. 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**.

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

5.1.3. 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;

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

5.1.5. 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 Limited, Express Towers 10th floor, Nariman point Mumbai – 400021. 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

7.1. All the manuals, guidelines, documents etc. provided by Client/company shall be treated as Confidential information by the Service Provider.

7.2. 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.

7.3. The service provider shall provide Reports, Documents and all other relevant materials, artifacts etc. during the assignments to ECGC Ltd. and ECGC Ltd. shall own

all IPRs in such Reports, Documents and all other relevant materials, artifacts etc. All documents related to such shall be treated as confidential information by the Bidder.

7.4. 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.

7.5. 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.

7.6. 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

7.7. A party shall not to 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. Non- Disclosure:

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

8.2. The service provider will use the Company's Confidential Information solely to fulfil its obligations as part of and in furtherance of this service contract.

8.3. The service provider shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Company or its subsidiaries or affiliates, and shall not disclose the Confidential Information to any unauthorized third party. The service provider shall not disclose any Confidential Information to any person except to its employees and consultants, on a need to know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms as restrictive as those specified in this Agreement. In this regard, any agreement entered into between the service provider and any such

person/s shall be forwarded to the Company promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the service provider shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information.

8.4. The service provider shall use the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information, and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use.

9. Damages/ Liability clause

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

10.1. 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 not 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.

10.2. 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.

10.3. Except for breach of Confidentiality and Infringement of Intellectual property rights under this agreement, each party's total 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 fees paid by the Company to the Service Provider under this Agreement.

10.4. 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.

10.5. 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.

10.6.

10.7. **Limitation of Liability**

The aggregate liability of Bidder or ECGC in connection with this Agreement/ service contract, the services provided by bidder for the specific scope of work document, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise) and including any or all liability shall be the total bid amount.

11. WARRANTY & WARRANTY DISCLAIMER

11.1. 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, RENEWAL AND TERMINATION

12.1. The term of this Agreement shall be for a period of 6 months ("**Term**"), commencing from the Effective Date.

12.2. In case of a breach (material in nature) under the Contract or any other subsequent documents containing obligations under the service agreement, the Company shall notify 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.

12.3. Upon expiry or termination 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.

13. Working on ECGC's Holiday

Request for permission for working on Saturday / Sunday / holidays if required, should be submitted 3 working days prior to the date of holiday, to respective locations 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. MISCELLANEOUS PROVISIONS

14.1. It is expressly agreed between the parties that the Contract, The Request for Tender (RFT) Document, any addendum or corrigendum issued thereafter and the complete Annexures thereto constitute the Entire Agreement between the Parties.

14.2. 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.

14.3. If either party is prevented from performing any obligation under this Agreement (excluding payment obligations) by causes beyond its control, including labor disputes, pandemic, civil commotion, war, governmental regulations or controls, casualty, inability to obtain materials or services or acts of God, such defaulting party will be excused from performance for the period of the delay and for a reasonable time thereafter.

14.4. 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/tender/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/tender/contract.

14.5. 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.

14.6. 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

14.7. This Agreement shall not be assigned by either party without the prior written consent of the other party.

14.8. 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.

14.9. 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.

14.10. 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.

14.11. This Agreement along with the said RFT, bids and other annexures constitutes the entire agreement between parties relating to the subject matter hereof and supersedes 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.

14.12. The courts at Mumbai shall alone have exclusive jurisdiction for the purposes of adjudication of any dispute of differences whatsoever in respect of or relating to or arising out of or in any way touching the RFT, the subsequent contract awarded or the terms and conditions of the Contract.

14.13. This Agreement may be executed in counterparts, which together will constitute one instrument.

14.14. **Force Majeure:**

Notwithstanding the provisions of Terms and Conditions of Contract, the Service Provider shall not be liable for liquidated 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.

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 : Shashank P. Bajpai	**NAME:**
DESIGNATION : CISO	**DESIGNATION:**

WITNESSES:

1. 2.

Annexure – A

Scope of Work & Deliverables Timeline

Background

ECGC intends to undertake a review of its adherence to the regulatory requirements of Insurance Regulatory and Development Authority of India (IRDAI) pertaining to Cyber Security.

Current State of Information Technology (herein after referred as IT) In ECGC

ECGC has the following IT applications in operation:

1. An Enterprise Resource Planning (ERP) System, supporting all Core Insurance and non-core functions of ECGC, including Enterprise Accounting and MIS.
2. A Public Portal, catering to the general public, offering information on ECGC's products and services, public disclosures, and company information.
3. A Client Portal, catering to Exporter and Banker clients.
4. A Grievance Management Portal, IGMS, as mandated by the regulator IRDAI, to manage customer complaints.
5. A Treasury software system, supporting the Treasury operations of ECGC.
6. A RBI-NDS system for supporting the Treasury operations of ECGC.
7. An Enterprise Email solution for all employees.
8. A web content filtering solution for employee browsing needs and to filter against malware.
9. A messaging security solution to filter malware and spam in emails.
10. An Antivirus solution for all servers and employee PCs.
11. A patch management solution for servers and employee PCs.
12. An Active Directory solution for single sign on (partial) and managing group policies.
13. A biometric system for managing employee attendance / reimbursements.
14. A swipe card system for some employees for access control to some office.
15. A Hypervisor solution for managing virtualization.

The above applications are supported by a SAN-based storage solution, multiple switches, and firewalls (virtualized). ECGC employees are connected to the various applications via a MPLS VPN and freshly rolled out SD-WAN. All major systems /

services used by employees are centralized. The management of the IT setup (DC & DRC) is outsourced to a third-party.

Purpose of Audit

ECGC envisages a review of its processes and IT infrastructure with respect to the following areas:

1. Review based on IRDAI Circular Ref No: IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 (Guidelines on Information and Cyber Security for Insurers) and amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020
2. ITGC (General Controls) Audit for IT systems handling Financial Information
3. Vulnerability Assessment and Penetration Testing of IT Systems

The auditor shall also assist ECGC Ltd. in the following areas pertaining to the IRDAI Circulars -

4. Adhering to changed or updated timelines of compliance
5. Adhering to further clarifications issued by IRDAI
6. Providing additional certification/s and clarifications as required by the IRDAI from the cyber security auditor

The audit will include but not limited to the testing of Applications, review of Information Security Policy & Procedures, Gap Assessment in IT security and Procedures, Assessment of Network Security & Information Security solutions, Vulnerability and Penetration testing, review of Data Centre including physical visits, compliance with IRDAI, and submission of reports. The backbone IT infrastructure of the Company is located at Mumbai and Data Centre at Faridabad.

Based on the approach mechanism and intended outcome the scope of work is outlined into two parts-

Part A: Systems and Process Audits and
Part B: Technical Cybersecurity VAPT Audit

The bidder has to undertake the following process audits with respect to Governance, Risk and Compliance under Part A

A.1. Cybersecurity Audit

A.2. IT Systems Audit

Following are key indicative but not exhaustive scope of work to be carried out by the selected Bidder -

A.1. Cybersecurity Audit

Review based on IRDAI Circular (Guidelines on Information and Cyber Security for Insurers) Ref No. IRDA/IT/GDL/MISC/082/04/2017 dated 07.04.2017 and amended vide its Ref. No: IRDA/IT/CIR/MISC/ 301/12/2020 dated 29/12/2020

IRDAI's information and cyber security guidelines and Annexure A (control checklist) covering all of the below areas but not limiting to -

1. Enterprise Security
2. Information Asset Management
3. System acquisition, development and maintenance
4. Information Security Risk Management
5. Data & Communication Security
6. Application, Mobile & Cloud Security
7. Cyber Security
8. Platform / Infrastructure Security
9. Network & Endpoint Security
10. Cryptography & Key Management
11. Security Logging & Monitoring
12. Virtualization
13. Information System Audit
14. Organization of information security
15. Human resource security
16. Access Control
17. Cryptography
18. Physical Access and Environmental controls
19. Operations security
20. Communication Security
21. Information security in supplier relationships

22. Information security incident management
23. Compliance with legal requirements
24. Business Continuity Management
25. Compliance
26. Cloud Security
27. Information and Cyber Security Policy
28. Cyber Security Assurance Programme

A.2. IT Systems Audit

Perform a review of the areas pertaining to IT General Controls and System readiness. The bidder shall incorporate this audit activity in parallel to above process audit and submit a separate Report on the same.

The areas are as mentioned below, however they are not limiting to -

1. Change Management
2. IT Governance
3. IT Strategy
4. Security Policy, Procedures and Frameworks
5. Incident & Problem Management
6. Backup Management
7. Access Management
8. Patch Management
9. Physical & Environmental Control
10. IT security risk assessments
11. Functionality review
12. IT landscape review
13. Review of IT operations
14. Review of information security
15. Review of third party suppliers and outsourcing
16. Review of design of Business Continuity (BC) and Disaster Recovery (DR)
17. Review of IT operations
18. Conduct walkthroughs and reviews of identified in-scope controls pertaining to the review areas in scope
19. Conduct meetings with relevant stakeholders to understand the process of capacity planning for applications and IT infrastructure
20. Obtain and review relevant evidences for each control

21. Perform sample based testing where relevant
22. Identify and document control gaps
23. Discuss identified gaps with stakeholders
24. Present reports for each of the above areas
25. Discuss and finalize the risk register with the IT Security function head - CISO
26. Suggest implementation guidelines based on the industry best standards & a prioritized roadmap to achieve the recommendations of the review report.

Key Stages of all the three A.1 and A.2 Process based Audits:

1. Kick-off Meeting & Stakeholder Identification
2. Audit Preparation on site & Related documentation to be shared
3. Audit Process
4. Prepare list of pre-requisites with respect to the above areas and share the same.
5. Conduct walkthroughs and reviews of identified in-scope controls pertaining to the review areas in scope
6. Obtain and review relevant evidences for each control
7. Perform sample based testing where relevant
8. Present reports for each of the above areas
9. Identify and document control gaps
10. Discuss identified gaps with stakeholders
11. Provide GAP analysis report and recommendations to address the identified the gaps.
12. Suggest implementation guidelines based on the industry best standards & a prioritized roadmap to achieve the recommendations of the review report.
13. Create roadmap for addressing identified gaps with prioritization
14. Create roadmap and strategy to address all identified shortcomings.
15. Prioritize the solution w.r.t. organization‘s posture (Immediate measures/long term measures)
16. Recommend the best fit solutions & controls
17. In collaboration with ECGC IT staff, resolve all the gaps identified in the gap analysis, vulnerabilities found, additional vulnerabilities pointed out by ECGC and make ECGC ready for final audit.
18. Perform the final Audit in lines to above scope
19. Draft Audit Report Generation & Discussion

20. Final Audit Report Submission, Discussion (Two separate Audit reports signed by CISA Auditor shall be submitted for A.1 & A.2 respectively)
21. Finalize the prioritized implementation roadmap
22. Re-assessment of Cyber Maturity Rating Scale and Final Ratings post the Audits

Part B: Technical Cybersecurity VAPT Audit

The bidder shall conduct technical testing on the IT Systems, OS, Applications and Network and report the vulnerabilities.

The scope of this Vulnerability Assessment – Penetration Testing Audit report is as below –

1. Internal Network Vulnerability Management
    a. 65(internal IPs)
2. External Black Box Network & Application PT
    b. 4(external IPs)
3. Web Application security testing (Black Box) must also include complete proof of exploit in all cases of all the reported vulnerabilities
4. ECGC websites should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) 2021 standard
5. The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website “Certified for Security”.
6. Auditor must test website for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/application.
    i. Vulnerabilities to SQL Injections
    ii. CRLF injections
    iii. Directory Traversal
    iv. Authentication hacking/attacks
    v. Password strength on authentication pages
    vi. Scan Java Script for security vulnerabilities
    vii. File inclusion attacks
    viii. Exploitable hacking vulnerable
    ix. Web server information security
    x. Cross site scripting

xi. PHP remote scripts vulnerability
xii. HTTP Injection
xiii. Phishing a website
xiv. Buffer Overflows, Invalid inputs, insecure storage etc. Any other attack that can be a vulnerability to the website or web applications.

7. ECGC websites should be audited as per the Industry Standards and also as per the latest OWASP (Open Web Application Security Project) 2021 standard
8. The auditor is expected to submit the recommendation, final audit report after the remedies/recommendations are implemented. The final report will certify the particular Website “Certified for Security”.
9. Auditor must test website for attacks. The various checks/attacks /Vulnerabilities should cover the following or any type of attacks, which are vulnerable to website/application.
    i. Vulnerabilities to SQL Injections
    ii. CRLF injections
    iii. Directory Traversal
    iv. Authentication hacking/attacks
    v. Password strength on authentication pages
    vi. Scan Java Script for security vulnerabilities
    vii. File inclusion attacks
    viii. Exploitable hacking vulnerable
    ix. Web server information security
    x. Cross site scripting
    xi. PHP remote scripts vulnerability
    xii. HTTP Injection
    xiii. Phishing a website
    xiv. Buffer Overflows, Invalid inputs, insecure storage etc. Any other attack that can be a vulnerability to the website or web applications.
    xv. Generate all security testing reports and provide recommendations.
    xvi. Suggest the best possible patching and remediation for the identified vulnerabilities.
    xvii. Discuss and document the management action plan with timeline to implement the recommendations on the same

xviii. In collaboration with ECGC IT staff, resolve all the gaps identified in the vulnerabilities assessment and penetration testing, and re-assess the vulnerability post closure of gaps.

xix. Provide final VAPT reports post re-validation testing of closed gaps.

NOTE:

1. The complete exercise including process audit and technical VAPT testing has to be done on premise at ECGC office only.
2. The bidder has to re-assess the existing Cyber Maturity Model-Rating score and provide the final ratings for current year, post the Audit.

THE OVERALL RESPONSIBILITY OF THE SERVICE PROVIDER IS TO ENSURE ECGC'S COMPLIANCE TO ALL REGULATIONS RELATING TO GUIDELINES ON INFORMATION AND CYBER SECURITY AS ISSUED BY IRDAI.

The Selected Bidder is expected to carry out its assignment with due diligence and in accordance with prevailing standards of the profession. The selected bidder has to make a project plan to deliver all Audit Reports within timelines and present the same to the ECGC Management. The bidder shall be free to merge common areas of review and carry-out sampling processes and walkthrough discussions in a non-repetitive manner.

The selected bidder shall be accountable and responsible for the services required to be performed and it shall not be an excuse that the employee/personnel or key person of the selected bidder committed mistakes or left the bidder during the continuance of the project as per this RFT or for any other reason whatsoever.

Deliverables with Timelines

Sl. No.	Deliverables	Expected Timelines
Part A		
1.	Final Cybersecurity Audit Report	2-3 Weeks
2.	Final IT Systems Audit Report	
Part B		
4.	VAPT Security Testing Reports	1-2 Weeks

List of Abbreviations used in the Scope of Work

S.No.	Abbreviation	Full Form / Remark
20.	ERP	ENTERPRISE RESOURCE PLANNING
21.	MIS	MANAGEMENT INFORAMTION SYSTEMS
22.	IGMS	INTEGRATED GRIEVANCE MANAGEMENT SYSTEM
23.	NDS	NEGOTIATED DEALING SYSTEM
24.	SAN	STORAGE AREA NETWORK
25.	MPLS	MULTI-PROTOCOL LABEL SWITCHING
26.	VPN	VIRTUAL PRIVATE NETWORK
27.	SD-WAN	SOFTWARE DEFINED WIDE AREA NETWORK
28.	BC-DR	BUSINESS CONTINUITY – DISASTER RECOVERY
29.	ITGC	INFORMATION TECHNOLOGY GENERAL CONTROLS
30.	IRMS	INVESTMENT RISK MANAGEMENT SYSTEMS
31.	IT	INFORMATION TECHNOLOGY
32.	URL	UNIFORM RESOURCE LOCATOR
33.	IRDAI	INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA
34.	CISC	CORPORATE INFORAMTION SECURITY COMMITTEE
35.	VA	VULNERABILITY ASSESSMENT
36.	PT	PENETRATION TESTING
37.	OS	OPERATNG SYSTEM
38.	DB	DATABASE SYSTEMS

Annexure – 8 : Bank Details

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 Company

(Company Seal)

Name :

Designation :

Contact No (Mobile)

Email Id