# GIC HOUSING FINANCE LTD.

**REQUEST FOR PROPOSAL**

**FOR**

**MANAGED CYBER SECURITY RISK ADVISORY SERVICES**

**FOR ONE YEAR**

**RFP Reference Number: REF: GICHF:2024-25/07,**

**Dt. 21-06-2024**

| ACTIVITY SCHEDULE | | |
|---|---|---|
| **S.NO.** | **ACTIVITY** | **DETAILS** |
| **1** | Release of RFP | 21-06-2024 |
| **2** | Address for Receipt/Submission of Bid document | GIC HOUSING FINANCE LTD National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020. |
| **3** | Bid Submission | **Sealed** - Technical & Commercial Bids in Hard Copy only. |
| **4** | Last Date & Time for submission | **05-07-2024**<br>**13:00 hrs.** |
| **5** | Bid Opening Date & Venue | **05th July, 2024**<br>**(**To be opened and evaluated internally at GICHFL Head Office). |
| **6** | Contact Details | **Mr. Bhavik Dedhia**<br>Chief Information Security Officer<br>Ph:9167091254 |
| **7** | E-mail ID | Bhavik.dedhia@gichf.com |

## 1. ABOUT GIC HOUSING FINANCE LTD:

GIC Housing Finance Ltd (GICHFL) is a company registered under Section 25 of the Companies Act, 1956 with its Registered Office at National Insurance Building, 6th Floor, 14, J. Tata Road, Churchgate, Mumbai – 400020 and its 72 Branch Offices across PAN India.

Our Promoters are General Insurance Corporation of India, The New India Assurance Company Ltd, United India Insurance Company Ltd, The Oriental Insurance Company Ltd and National Insurance Company Ltd.

## 2. OBJECTIVE OF RFP:

The objective of this RFP is to solicit proposals from qualified vendors to provide Managed Services for Cyber Security Risk Advisory for GIC Housing Finance Ltd. We aim to engage a partner who can help us mitigate cyber security risks, enhance our security posture, and ensure compliance with industry standards and regulations.

## 3. MINIMUM ELIGIBILITY CRITERIA FOR BIDDER:

In order to qualify for bid, bidder should satisfy following eligibility criteria. Following format to be filled by the bidder and must submit in Envelope A in its order along with relevant documentary proof.

| Sr. No | Specific Requirement | Documents Required | Bidder's Response along with Details of supporting documents |
|---|---|---|---|
| 1. | The bidder must be a Company/LLP/Partnership Firm incorporated in India and registered under the Companies Act 2013 or Limited Liability Partnership Act 2008 or Partnership Act 1932 as applicable and must have a registered office in India for at least 5 years. | • Copy of Certificate of Incorporation / Registration | |
| 2. | Firm should have all necessary licenses, permissions, consents, No Objections, approvals as required under law for carrying out its business. Bidder should have valid GST and other applicable taxes registration certificates /PAN etc. | An undertaking to be submitted along with copy of Pan card and GST Registration certificate | |

| | | | |
|---|---|---|---|
| 3. | The bidder should be ISO27001:2013/2022 certified. | Copy of a valid certificate should be attached. | |
| 4. | The Bidder should have experience in managing similar kind of projects in at least two Financial Institution / NBFC / Public Sector Bank /Government Organization / Large Corporates in India not older than 3 years. | An undertaking from the vendor on the company letter head or a document certifying the same is to be produced with clients list attached. | |

## 4. SCOPE OF WORK:

The primary objectives of this engagement include:

A. Conducting a comprehensive security gap assessment of our current information security landscape.

B. Developing a comprehensive information security strategy & framework to protect assets, detect and respond to threats, and ensure regulatory compliance and data security / privacy.

C. Provide support and guidance to IT /IS teams during implementation of security recommendations and remediation measures and function as internal risk advisory.

D. Assist organization for ensuring compliance with relevant regulatory requirements (RBI, IRDAI, NHB, Cert-In, etc.) and adoption of relevant industry standards (NIST, ISO 27001, CIS Controls etc.)

The scope of work for tenure of one year includes, but is not limited to:

### I. Cyber Security Posture Assessment:

- Conduct a thorough evaluation/ assessment of the organization's cyber security landscape.
- Identify and analyze risks associated with current cyber security / IT practices.
- Assess compliance with industry best practices and regulatory standards such as NIST Framework, ISO27001, ISO22301, IRDAI circulars, RBI guidelines, and NHB regulations.
- Provide comprehensive gap analysis highlighting areas for improvement along with technological and process gaps.

- Developing a comprehensive information security strategy & framework to protect assets, detect and respond to threats, and ensure regulatory compliance and data security & privacy.

Frequency – One Time

Deliverables –

A. Information Security Posture Report: Comprehensive evaluation of the organization's current cyber security landscape, detailing identified risks and areas of concern.
B. Gap Analysis Report: Identification of technological and process gaps, with actionable improvement plan along with closure support.
C. Information Security Strategy & Framework for the organization.
D. Executive Management Presentation.

## II. Security Architecture Review:

- Review network diagrams, system designs and architecture documentation.
- Conduct a comprehensive analysis of security controls implemented within the network infrastructure.
- Assess the effectiveness of access controls, segmentation and encryption mechanisms.
- Identify potential vulnerabilities resulting from misconfigurations or architectural flaws.
- Recommend architectural enhancements to improve resilience and mitigate risks.

Frequency – One Time

Deliverables –

Network Architecture Report with Recommendations for Architectural enhancement to improve resiliency and mitigating flaws. Detailed Network Diagrams and architecture for the organization to be provided along with suggestions on network segmentation.

## III. Cloud Security Assessment:

- Evaluate security controls and configurations of cloud services and infrastructure.
- Mitigate risks associated with cloud adoption.
- Ensure compliance with industry standards and regulatory requirements.
- Provide guidance on secure cloud configuration and governance practices.

Frequency – One Time

Deliverables –

A. Cloud Security Assessment report with recommendations.

B. Risk Mitigation Plan for Cloud Adoption.
C. Secure Cloud Configuration Guide.

## IV. Configuration Reviews:

- Perform detailed configuration reviews for various systems and devices against security best practice on sample basis including Desktops (10), Laptops (15), Firewall (10), SD WAN (10), Wi-Fi controllers (2), Servers (20) (On-Premises and On-Cloud), Backup systems, Databases (10) and other solutions.
- Provide detailed recommendations for improving configurations to align with security best practices and formation of hardening baselines for different devices.
- Review and suggest improvements for Firewall rules.

Frequency – Bi-Annually

Deliverables –

A. Configuration Review reports and Firewall Rule Review Report.
B. Recommendations for Configuration Improvements.
C. Hardening Baselines for Various Devices and Solutions.

## V. Active Directory Review:

- Conduct bi-annual reviews of Active Directory configurations.
- Analyze Active Directory configurations, group policies and domain trust relationships.
- Assess user account management practices, including password policies and authentication mechanisms.
- Review privileged access controls and administrative delegation.
- Identify security risks such as outdated software versions or misconfigured permissions.
- Recommend remediation actions to enhance Active Directory security posture.

Frequency – Bi-Annually

Deliverables – Active Director Assessment Report with recommendations.

## VI. Incident Response Training & Table-top Exercise:

- Conduct bi-annual training sessions to incident response teams on incident detection, containment, eradication, and recovery procedures.
- Develop customized incident response playbooks and procedures for different types of security incidents along with Cyber Crises Management Plan.

- Conduct table top exercises to simulate real-world security incidents and test the effectiveness of response plans.
- Provide assistance in planning for IT DR Drills and oversee DR setup functions as planned for meeting defined RTO / RPO.
- Review and update incident response plans based on lessons learned from training exercises.

Frequency – Bi-Annually

Deliverables –

A. Incident Response Training.
B. Cyber Crises Management Plan along with Incident Response Playbooks catering different incident scenarios.
C. Conduction of Table-Top Exercises.

## VII. Policy and Procedure Development:

- Conduct review of existing Security and IT policies, procedures and guidelines.
- Identify gaps and inconsistencies in existing policy / procedures with industry standards and regulatory requirements and rectify the existing policies / procedures in alignment with the same.
- Develop new policies and procedures to address emerging threats, technology changes, organizational needs, industry frameworks and regulatory compliance.
- Provide training and awareness sessions to ensure employees understand and adhere to security policies and procedures.
- Creation of other documents like Risk Register / Exception handling form.

Deliverables –

Policies and Procedures customized to GICHFL with alignment to industry and regulatory compliance.

## VIII. Additional Activities and Assessments:

- Assist in setting up server for collecting logs to ensure CERT-in compliance.
- Conduct user access reviews for applications / systems. Review the adherence to access provisioning/ de-provisioning processes
- Review the backup configuration / frequency to ensure all critical assets are covered as part of the schedule. Review the backup restoration test results.
- Review patch compliance for Infrastructure (Server, Endpoint, Network Devices)

- Track any exceptions to the information security posture in the organization.

## 5. MANAGED SERVICES:

The vendor is required to deploy on-site and remote shared resources with the appropriate industry experience and security certifications. These resources must be capable of achieving the objectives and scope of work outlined in this RFP and facilitating effective collaboration and communication with stakeholders.

Roles & Responsibilities:

A. Timely Delivery Assurance: Develop a detailed project plan with milestones and deadlines for all deliverables. Conduct regular progress reviews and adjust plans as necessary to stay on track.

B. Monitoring and Follow-ups: Continuously monitor the progress of security tasks and initiatives. Follow up with internal teams to ensure timely completion of assigned tasks. Coordinate with external vendors to ensure they meet their security obligations and resolve any issues promptly. Establish regular check-ins and status meetings to track progress and address any blockers.

C. Reporting and Documentation: Prepare and deliver detailed presentations, reports, and briefing notes to management and relevant committees. Regularly update stakeholders on the current cyber security posture and ongoing security activities.

D. Governance, Risk, and Compliance (GRC) Management: Maintain the GRC Dashboard/Tracker for all open observations and risks identified in internal and external audits. Ensure all risks are assessed, prioritized, and managed according to the company's risk management framework. Regularly review and update risk management and compliance documentation.

E. Guidance and Collaboration: Offer support and guidance to IT and IS teams during the implementation of security recommendations and remediation measures. Facilitate collaboration and communication between various stakeholders to ensure alignment on security goals and initiatives.

## 6. PROPOSAL REQUIREMENTS:

Bidders are required to submit a proposal that includes the following:

A. Company Overview
   - Background and history of the company.
   - Experience in providing cyber security risk advisory services.
   - Key differentiators and unique value propositions.

B. Approach and Methodology
   - Detailed description of the approach to be used in delivering the services.

C. Team Composition
   - Profiles of the team members who will be assigned to the project.
   - Relevant qualifications and experience.

D. Case Studies and References
   - Examples of similar projects completed.
   - Client testimonials and references.

## 7. SUBMISSION INSTRUCTIONS:

Two sealed Envelops in Hard Copy to be submitted:

### A. Envelope 'A'

The envelope shall be sealed and marked as "Envelope A-Tender for Managed Cyber Security Risk Advisory Services for GIC Housing Finance Ltd" in the top left hand corner. The envelope shall be dated with the current date in the top right hand corner.

It should contain following:

i. Minimum Eligibility Criteria table for Bidder and its supporting documents as specified in Section 3 of RFP.
ii. Proposal Requirements as mention in Section 6 of this RFP.

### B. Envelope 'B'

The envelope shall be sealed and marked as "Envelope B-Tender for Managed Cyber Security Risk Advisory Services for GIC Housing Finance Ltd" in the top left hand corner. The envelope shall be dated with the current date in the top right hand corner.
Please note that no other information other than the commercials should be furnished in this envelope.

Format for commercial bid is attached in Annexure A.

## 8. EVALUATION AND SELECTION CRITERIA:

A. Technical Evaluation Criteria:

| Sr. No | Parameters | Marks |
|---|---|---|
| 1 | Expertise and experience in cyber security risk advisory | 25 |
| 2 | Quality and comprehensiveness of the proposal. Proposed methodology and approach | 30 |
| 3 | References and case studies. | 20 |
| 4 | Team qualifications | 25 |

B. Example on Selection Criteria:

The weightage of the technical bids and financial bids is kept as 80:20. In response to the RFP, say 4 proposals, A, B, C & D were received. The consultancy evaluation committee awarded them 85, 80, 75 and 60 marks for the technical bid respectively, thereby ranking them as T-1, T-2, T- 3 and T-4 respectively.
The financial proposals of technically ranked bidders, i.e. T-1, T-2, T-3 and T-4 were opened.

| Proposal | Evaluated cost |
|---|---|
| A | Rs. 120 |
| B | Rs.100 |
| C | Rs. 110 |
| D | Rs.130 |

The consultancy evaluation committee examined the financial proposals and evaluated the quoted prices as under:

Proposal Evaluated cost
A) Rs.120
B) Rs.100
C) Rs.110
D) Rs. 130

Using the formula LEC / EC, where LEC stands for lowest evaluated cost and EC stands for evaluated cost, the committee gave them the following points (rounded to nearest two decimal places) for financial proposals:
A: 100 / 120 = 83.33 points
B: 100 / 100 = 100.00 points
C: 100 / 110 = 90.91 points
D: 100 / 130 = 76.92 points

In the combined evaluation, thereafter, the evaluation committee calculated the combined technical and financial score as under:
Proposal A: 85x0.80 + 83.33x0.20 = 84.67 points.
Proposal B: 80x0.80 + 100.00x0.20 = 84.00 points
Proposal C: 75x0.80 + 90.91x0.20 = 78.18 points.

Proposal D: 60x0.80 + 76.92x0.20 = 63.38 points.

The three proposals in the combined technical and financial evaluation were ranked as under:
Proposal A: 84.67 points: H-1
Proposal B: 84.00 points: H-2
Proposal C: 78.18 points: H-3
Proposal D: 63.38 points: H-4

Proposal A at the evaluated cost of Rs.120 was, therefore, declared as winner.

**Notification of Award/Purchase Order:**

After selection of the H1 bidder and after obtaining internal approvals, GICHFL will send Notification of Award/Purchase Order to the selected Bidder.

**Signing of Purchase Order:**

- Within 2 days of receipt of Purchase order the successful Bidder shall accept and acknowledge the Purchase Order.
- Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

**Termination of contract with selected bidder:**

GICHFL reserves the right to terminate the contract with the selected Bidder by providing a 30 days' prior written notice. Termination may occur for any reason, including but not limited to the Bidder's incapability to provide standard services or due to negligence on the part of the Bidder.

## 9. PAYMENT SCHEDULE:

A. **Initial Payment:**
- 10% of the total contract value will be paid upon Contract Signing and project kick-off, against the corresponding invoice.

B. **Quarterly Payments:**
- The remaining payments will be disbursed on a quarterly basis.
- Payments will be made after the deliverables for each quarter are successfully achieved and verified by GICHFL.

C. **Bidder Responsibilities:**
- Develop a comprehensive approach and methodology to achieve the scope of work and objectives outlined in this RFP.

- Plan and divide project activities on a quarterly basis, ensuring clear milestones and deliverables for each quarter.
- Ensure all quarterly deliverables are completed to facilitate timely payment.

## 10. AUDIT REQUIREMENTS:

GICHFL is subjected to various audits [internal / statutory / RBI etc.]. In the event of any observation by the audit regarding security, access etc., the same will be intimated to the Bidder. The Vendor to carry out the changes for enabling GICHFL to comply on the same, if required. No additional cost would be paid by GICHFL.

## 11. RIGHT TO AUDIT:

Compliance with security best practices may be monitored by various periodic security audits performed by or on behalf of the Company. The periodicity of these audits will be decided at the discretion of the Company. These audits may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, security controls and program change controls. To the extent that the Company deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the selected bidder shall afford the Company's representatives access to the selected bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The selected bidder must provide the Company access to various monitoring and performance measurement systems (both manual and automated). The Company has the right to get the monitoring and performance measurement systems (both manual and automated) audited without prior approval/notice to the selected bidder.

## 12. OTHER TERMS & CONDITIONS:

- Right to Terminate the Process: GICHFL may terminate the RFP process at any time and without assigning any reason. GICHFL makes no commitments, express or implied, that this process will result in a business transaction with anyone.
- This RFP does not constitute an offer by GICHFL. The Bidder's participation in this process may result GICHFL selecting the Bidder to engage towards execution of the subsequent contract.
- GICHFL reserves the right to reject any or all proposals.
- The Bidders should ensure that all assumptions/clarifications required are clarified beforehand. Any bids with words/phrases such as (but not limited to) "assumption", "it is understood that", "conditional offer" may be subjected to rejection at any stage of evaluation.
- Please note that prices should not be indicated in the technical proposal but should only be indicated in the commercial proposal. However, a masked bill of material masking the price information be provided along with the technical proposal.

- The two sealed envelope containing copies of technical Proposal and commercial Proposal, clearly marked “Tender for Managed Cyber Security Risk Advisory Services for GIC Housing Finance Ltd”.
- This RFP does not commit GICHFL to award a contract or to pay any costs incurred in the preparation of a proposal.
- The outer envelope thus prepared should also indicate clearly the name, address, telephone number and E-mail ID of the Bidder to enable the Bid to be returned unopened in case it is found to be received after the time and date of Proposal submission prescribed herein.
- All the pages of the Proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bidder’s Proposal.
- The original Proposal shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initialed by the authorized signatory of the Bidder.
- All pages of the bid shall be initialed and stamped by the authorized signatory of the Bidder.
- The Bidder must submit a certificate of undertaking on its official letter-head duly signed by its authorized signatory confirming the acceptance of all the terms & conditions contained in and spread throughout this Bid Document.
- All information provided by GICHFL in this RFP is confidential and must be treated as such by the bidders.
- Decision as to any arithmetical error, manifest or otherwise in the response to Bid Document shall be decided at the sole discretion of GICHFL and shall be binding on the Bidder. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder. Bidder should be a legal entity and financially solvent. Bidder must warrant that no legal action is pending against them in any legal jurisdiction which affects its ability to deliver the RFP requirements.
- GICHFL reserves the right to re-issue/re-commence the entire bid process in case of any anomaly, irregularity or discrepancy in regard thereof. Any decision of GICHFL in this regard shall be final, conclusive and binding on the Bidder.
- Modification to the RFP, if any, will be made available as an addendum on GICHFL website/will be emailed to bidder.

# ANNEXURE A

**FORMAT FOR COMMERCIAL BID:**

| Sr. No | Activity | Total Price (INR) Exclusive of Taxes |
|---|---|---|
| 1 | Cyber Security Posture Assessment | |
| 2 | Security Architecture Review | |
| 3 | Cloud Security Assessment | |
| 4 | Configuration Reviews | |
| 5 | Active Directory Review | |
| 6 | Incident Response Training & Table Top Exercise | |
| 7 | Policy & Procedure Development | |
| 8 | Additional Activities & Assessments | |

**Applicable Taxes: _____ (% GST), please indicate applicable taxes.**

----------END OF RFP DOCUMENT----------