REQUEST FOR PROPOSAL

IT SECURITY AUDIT
AND
IPv6 COMPLIANCE AUDIT

GENERAL INSURANCE CORPORATION OF INDIA

Reference No. : ITMG / 69 / 2013-14

भारतीय साधारण बीमा निगम

Table of Contents

General Insurance Corporation of India
(A Government of India Undertaking)
'Suraksha', 170, J. Tata Road, Churchgate
Mumbai – 400020

Request for Proposal (RFP)
FOR
IT Security Audit

Introduction

The purpose of this RFP is to identify and select an appropriate vendor to assist GIC in doing an audit of its Outsourced DC and DR site, Network security architecture, Local Area network, remote access to GIC's network and other related services as per the Scope of work specified in **Annexure I**. The selected vendor shall engage with GIC in identifying the gaps and assist, guide, develop and render expert advice to GIC of India to ensure that its information assets are adequately protected on a continuous basis from a variety of threats such as error, fraud, embezzlement, sabotage, terror, extortion, espionage, privacy violation, service interruption and natural disaster.

About GIC

General Insurance Corporation of India is the sole designated Indian reinsurer. GIC provides reinsurance to the direct general insurance companies in the Indian market. GIC is spreading its wings to emerge as an effective reinsurance solutions partner for the Afro-Asian region and has started leading the reinsurance programmes of several insurance companies in SAARC countries, South East Asia, Middle East and Africa.

Existing Infrastructure.

GIC of India operates mainly from its Office in Mumbai, though it has branch offices in all the metros and overseas. The entire IT infrastructure of GIC can be summarized as having 40 plus servers and roughly about 550 PCs, 100 laptops spread over 6 floors of "Suraksha" building. The details of the hardware, software and networking equipments are as per **Annexure II**.

Bid Collection and Submission.

Tender Reference number	
Earnest Money Deposit (EMD)	Rs. 50,000/-
Date of commencement of sale of tender document	20.09.2013
Queries to be mailed to	itmg@gicofindia.com
Last Date and Time for receipts of tender offers	10.10.2013 up to 14.30 hours
Time and Date of Opening of technical bids	10.10.2013 at 15.00 hours
Place of Opening tender offers	Will be communicated in due course.
Address for Communication	General Insurance Corporation of India, 170, Suraksha, J Tata Road, Churchgate, Mumbai – 400020
Contact Telephone Numbers	Phone : 022 22867156 022 22867116 022 22867114

Tender offers will be opened in the presence of the bidder representatives who choose to attend the opening of tender on the above-specified date, time and place.

Contract Period :

Vendor should provide in-scope services to GIC for a period of three (3) years from the date of commissioning. The contract would initially be for a period of three years to be renewed on an annual basis at the option of GIC.

Eligibility Criteria :

GIC Re will first scrutinize the eligibility of the prospective bidders as per "Minimum Eligibility criteria" mentioned below. The offers of the bidders who fulfill the minimum eligibility criteria will be taken up for further scrutiny i.e technical evaluation**.**

Minimum Eligibility Criteria
Following criteria has been defined for minimum eligibility of firm:

- The firm should be empanelled with CERT-IN for the period 2012-2015.
- The organizations already providing IT related service(s) to GIC are not eligible to participate in this tender.

The documentary evidence in respect of above is essential. Technical bids not accompanied by documentary evidence are liable to be rejected.

Tender Procedure

1. **Two Bid System Tender**

THREE COPIES of Technical & Commercial bid (each in separate envelopes super scribed Original, First Copy & second Copy) must be submitted at the same time, giving full particulars at the address given below, on or before the schedule given above. All envelopes should be securely sealed and stamped.

These sealed envelopes containing the Technical and Commercial offer in triplicate should be together enclosed in a larger envelope duly sealed and marked.

2. **Late Tender offers**

Any tender offer received by Corporation after the deadline for submission of tender offer prescribed by the Corporation will be summarily rejected.

3. **Offer validity Period**

The offer should hold good for a period of **90 days** from the date of the opening of tender.

4. **Address of Communication**

Offers should be addressed to the following officer at the address given below:

Assistant General Manager (ITMG)
General Insurance Corporation of India,
Suraksha, 170, J Tata Road,
Churchgate, Mumbai – 400020.

5. **Modification and Withdrawal of Offers**

Modification or Withdrawal of Offers is not permissible after its submission. If the offer is withdrawn before the validity period, the EMD will stand forfeited.

6. **Opening of Offers**

Tender offers received within the prescribed closing date and time will be opened on 10.10.2013 at 15:00 hrs, in the presence of vendor or their representatives who choose to attend the opening of the tender on the specified date and time as mentioned earlier in the tender document. The vendor's representatives present shall sign a register of attendance and shall have authority to take decisions.

GIC, reserves the right to redefine the **scope of work** after opening the Technical Offers. In such a case, the revised scope of work shall be communicated to the bidders and the bidders shall be asked to submit the commercial offers on the same within next 5 working days.

7. **Hand written documents, Erasures or Alterations**

Complete and correct technical information of the product being offered must be filled in. The offers containing erasures or alterations will not be considered unless the same are authorized by affixing the company seal and signed by an authorized person.

8. **Short-listing of Vendors**

The Corporation will create a short-list of technically qualifying vendors and the commercial offers of only these vendors will be opened.

Procedure for Processing the Tender

a) Technical Bids would be opened first.
b) Technical evaluation will be done based on the following parameters :
    - Qualifications and Competence of Proposed Key Staff for the project (15 marks)
    - Adequacy of Methodology and work plan (25 marks)
    - IPv6 Readiness Audit experience & project plan (10 marks)
    - All bidders will get 50 marks for being Cert-in empanelled.

c) Commercial bids would be opened of only those respondents who have qualified in the Technical analysis. There will be a cutoff percentage of 75% for qualifying technically.
d) The commercially L1 vendor shall be identified out of the technically qualified bidders.

This procedure is subject to changes and the procedure adopted by GIC for opening the tender shall be final and binding on all the parties.

Technical evaluation:

GIC will scrutinize the technical offers. It will determine whether the technical details along with documents have been furnished as per RFP. The bidders who qualify in technical evaluation will only be short-listed for commercial evaluation. The technical evaluation will be done on the basis of the information provided in the "Bidder's Information" as per **Annexure III** format along with supporting documents. The bidder will have to provide a write up on the following points as a part of the technical evaluation.

1. Project Plan.
2. Implementation methodology
3. Audit tools
4. Audit period
5. Deliverables
6. Audit Team details such as qualifications, experience etc. as per **Annexure IV**
7. Case study of any of the similar audits carried out in the past

Commercial evaluation.

GIC will open and scrutinize the commercial offers of the technically qualified bidders only. The Commercial bids will have to be submitted in the format as per **Annexure V**. Commercial bids should not have any alteration or overwriting. GIC may reject or load the financial implication of any alteration, if found into the commercial bid submitted by the respective bidder. The calculation arrived by GIC will be final and will be binding on the bidders. If any cost items in the commercial bid is found to be blank and not filled with any amount then it shall be considered as zero and the same will be offered to GIC free of any charges. The commercially L1 vendor will be identified out of the technically qualified bidders.

Clarification of Offers

To assist in the scrutiny, evaluation and comparison of offers, GIC may, at its discretion, ask some or all bidders for clarification of their offer. The request for such clarifications and the response will necessarily be in writing.

No Commitment to Accept Lowest or Any Tender

GIC shall be under no obligation to accept the lowest or any other offer received in response to this tender notice and shall be entitled to reject any or all offers including those received late or incomplete offers, without assigning any reason whatsoever. GIC reserves the right to make any changes in the terms and conditions of the RFP. GIC will not be obliged to meet and have discussions with any bidder, and or to listen to any representations.

9. **Security Deposit**

Successful Vendor will have to sign an Agreement Contract with Corporation & submit Security Deposit equal to **10% of the Order value** in the form of a Bank Guarantee from any Nationalised or Scheduled Bank, valid for the period covering complete deliverables and 30 days thereafter.

This Security Deposit will be forfeited if the deliverables are not carried out as specified in the tender.

10.**Earnest Money Deposit (EMD)**

a) Bidders are required to submit **Earnest Money Deposit (EMD) of Rs. 50,000 (Rupees Fifty thousand only)** in the form of Bank Guarantee or through RTGS / NEFT into the account of "General Insurance Corporation of India" as per details below:

Sr. No.	**Details of Bank Account**	
1	Type of Account	Current
2	Account Number	001020100010245
3	Name of the Bank	Bank of India
4	Name of the Branch	Churchgate, Mumbai
5	Address of Branch	Eros Building, Churchgate, Mumbai – 400 020
6	MICR Code No.	400013014
7	IFSC Code No.	BKID0000010

b) Bidder must pay required EMD through RTGS / NEFT only, payment of EMD by any other mode like DD / Pay Order will not be accepted. Offers made without E.M.D. will be rejected.

The EMD made by the tender bidder will be forfeited if the bidder –

- Withdraws the tender bid after acceptance by GIC; or
- Withdraws the tender bid before the expiry of the validity period of the tender; or
- Violates any of the provisions of the terms and conditions of the tender.

The earnest money deposit is non-interest bearing and is refundable to unsuccessful tenderers.

The successful tenderer's EMD will be either discharged upon the tenderer executing the Contract or furnishing the Security Deposit.

Earnest Money Deposit must accompany all tender offers as specified in this tender document. EMD amount/Bank Guarantee in lieu of the same should not be mixed with Technical/Commercial bid. It should be in separate cover to be handed over to the department.

Delay in Information Security Audit

The Information Security Auditor must strictly adhere to the audit schedule, as specified in the Contract, executed between GIC and the Information Security Auditor, pursuant hereto, for performance of the obligations arising out of the contract and any delay will enable GIC to resort to any or all of the following at sole discretion of GIC.

(a) Claiming Liquidated Damages
(b) Termination of the agreement fully or partly

In addition to the termination of the agreement, GIC reserves the right to appropriate the damages from the earnest money deposit (EMD) given by the bidder or invoke GIC Guarantee given in lieu of EMD and/or invoke GIC guarantee given by the bidder against the advance payment.

Liquidated Damages

The liquidated damages will be an estimate of the loss or damage that GIC may have suffered due to delay in performance of the obligations (under the terms and conditions of the contract) by the Information Security Auditor and the Information Security Auditor shall be liable to pay GIC as liquidated damages at the rate of 1% per week delay, subject to a maximum of 5% of total cost of the project, for the delays attributable to the firm. If the delay exceeds five weeks, GIC reserves the right to cancel the order unconditionally.

Without any prejudice to GIC's other rights under the law, GIC shall recover the liquidated damages, if any, accruing to GIC, as above, from any amount payable to the Information Security Auditor either as per the Contract, executed between GIC and the Information Security Auditor pursuant hereto or under any other Agreement/Contract, GIC may have executed/shall be executing with the Information Security Auditors.

Indemnity

The Information Security Auditor shall, at their own expense, defend and indemnify GIC against any claims due to loss of data / damage to data arising as a consequence of any negligence during Information Security Audit.

Publicity

Any publicity by the bidder in which the name of General Insurance Corporation is to be used should be done only with the explicit written permission of General Insurance Corporation.

Force Majeure

The Information Security Auditor or GIC is not responsible for delays or nonperformance of any contractual obligations, caused by war, blockage, revolutions, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, plague or other epidemics, fire, flood, obstructions of navigation by ice of port of dispatch, acts of Govt. or public enemy or any other event beyond the control of either party which directly, materially and adversely affect the performance of any contractual obligation.

If a force majeure situation arises, the Information Security Auditor shall promptly notify GIC in writing of such conditions and the change thereof. Unless otherwise directed by GIC, in writing, the Information Security Auditor shall continue to perform his obligations under the contract as far as reasonably practiced and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

Resolution of Disputes

General Insurance Corporation and the bidder shall make every effort to resolve amicably, by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the contract. If after thirty days from the commencement of such informal negotiations, General Insurance Corporation and the Bidder are unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution by formal arbitration.

All questions, disputes or differences arising under and out of, or in connection with the contract, shall be referred to two Arbitrators: one Arbitrator to be nominated by General Insurance Corporation and the other to be nominated by the Bidder. In the case of the said Arbitrators not agreeing, then the matter will be referred to an umpire to be appointed by the Arbitrators in writing before proceeding with the reference. The award of the Arbitrators, and in the event of their not agreeing, the award of the Umpire appointed by them shall be final and binding on the parties. **THE ARBITRATION AND RECONCILIATION ACT 1996** shall apply to the arbitration proceedings and the venue & jurisdiction of the arbitration shall be at Mumbai.

Privacy and Security Safeguards

The successful Bidder shall not publish or disclose in any manner, without GIC's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any location. The successful Bidder shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user (such as being reassigned, removed for repair, replaced, or upgraded) are cleared of all data and sensitive application software. The successful Bidder shall also ensure that all subcontractors who are involved in providing such security safeguards or part of it shall not publish or disclose in any manner, without GIC's prior written consent, the details of any security safeguards designed, developed, or implemented by the successful Bidder under this contract or existing at any location.

Confidentiality

• "Confidential Information" means any and all information that is or has been received by a party ("**Receiving Party**") from the other ("**Disclosing Party**") and that:

a) relates to the Disclosing Party;

b) is designated by the Disclosing Party as being confidential or is disclosed in circumstances where the Receiving Party would reasonably understand that the disclosed information would be confidential; or

c) is prepared or performed by or on behalf of the Disclosing Party by its employees, officers, directors, agents, representatives or consultants;

d) Without limiting the generality of the foregoing, Confidential Information shall mean and include any information, data, analysis, compilations, notes, extracts, materials, reports, drawings, designs, specifications, graphs, layouts, plans, charts, studies, memoranda or other documents, or materials relating to the licensed software, the modules, the program documentation, the source codes, the object codes and all enhancements and updates, services, systems processes, ideas, concepts, formulas, methods, know how, trade secrets, designs, research, inventions , techniques, processes, algorithms, schematics, testing procedures, software design and architecture, computer code, internal documentation, design and function specifications, product requirements, problem reports, analysis and performance information, business affairs, projects, technology, finances (including revenue projections, cost summaries, pricing formula), clientele, markets, marketing and sales programs, client and customer data, appraisal mechanisms, planning processes etc. or any existing or future plans, forecasts or strategies in respect thereof;

e) "Confidential Materials" shall mean all tangible / intangible materials containing Confidential Information, including, without limitation, written or printed documents and computer disks or tapes or any electronic form, whether machine or user readable;

f) Information disclosed pursuant to this clause will be subject to confidentiality for the term of contract plus two years;

g) Nothing contained in this clause shall limit the Successful Bidder from providing similar services to any third parties or reusing the skills, know-how and experience gained by the employees in providing the services contemplated under this clause, provided further that the Successful Bidder shall at no point use GIC's confidential information or Intellectual property.

• The Receiving Party shall, at all times regard, preserve, maintain and keep as secret and confidential all Confidential Information and Confidential Materials of the Disclosing Party howsoever obtained and agrees that it shall not, without obtaining the written consent of the Disclosing Party:

a) Disclose, transmit, reproduce or make available any such Confidential Information and materials to any person, firm, Company or any other entity other than its directors, partners, advisers, agents or employees, sub-contractors and contractors who need to know the same for the purposes of maintaining and supporting the Software provided as a part of Project. The Receiving Party shall be responsible for ensuring that the usage and confidentiality by its directors, partners, advisers, agents or employees, sub-contractors and contractors is in accordance with the terms and conditions and requirements of this Agreement; or

b) Unless otherwise agreed herein, use any such Confidential Information and materials for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its customers or their projects.

• In maintaining confidentiality hereunder the Receiving Party on receiving the confidential information and materials agrees and warrants that it shall:

a) Take at least the same degree of care in safeguarding such Confidential Information and materials as it takes for its own confidential information of like importance and such degree of care shall be at least, that which is reasonably calculated to prevent such inadvertent disclosure;

b) Keep the Confidential Information and Confidential Materials and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;

c) Limited access to such Confidential Information and Confidential Materials to those of its directors, partners, advisers, agents or employees, sub-contractors and contractors who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees, sub-contractors and contractors so involved to protect the Confidential Information and materials in the Confidential Manner prescribed in this Agreement; and

d) Upon discovery of any unauthorized disclosure or suspected unauthorized disclosure of Confidential Information, promptly inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Confidential Information and Confidential Materials, in whatsoever form, including any and all copies thereof.

• The Receiving Party who receives the Confidential Information and materials agrees that on receipt of a written demand from the Disclosing Party:

a) Immediately return all written Confidential Information, Confidential Materials and all copies thereof provided to, or produced by it or its advisers, as the case may be, which is in Receiving Party's possession or under its custody and control;

b) To the extent practicable, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the Disclosing Party;

c) So far as it is practicable to do so immediately expunge any Confidential Information relating to the Disclosing Party or its projects from any computer, word processor or other device in its possession or under its custody and control; and

d) To the extent practicable, immediately furnish a certificate signed by its director or other responsible representative confirming that to the best of his/her knowledge, information and belief, having made all proper enquiries the requirements of the clause of confidentiality have been fully complied with.

• The restrictions in the preceding clause shall not apply to:

a) Any information that is publicly available at the time of its disclosure or becomes publicly available following disclosure (other than as a result of disclosure by the Disclosing Party contrary to the terms of this Agreement); or any information which is independently developed by the Receiving Party or acquired from a third party to the extent it is acquired with the valid right to disclose the same.

b) Any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, statutory or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the Disclosing Party of such requirement with a view to providing the Disclosing Party an opportunity to obtain a protective order or to contest the disclosure or otherwise agree to the timing and content of such disclosure.

c) The Confidential Information and materials and all copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party and its disclosure hereunder shall not confer on the Receiving Party any rights whatsoever beyond those contained in this Agreement.

d) The confidentiality obligations shall survive the expiry or termination of the Agreement between the Successful Bidder and GIC and for a further period of two years thereafter.

Payment Terms:

Payment terms shall be as follows:

100% against delivery and completion after the submission of deliverable and proper sign off at the end of each phase as listed below:

Phase No.	Phase Description	Payment Schedule
1	Information Security Audit – 1st Year IPv6 Audit	100% payment on completion of Phase -1
2	Review Audit – 2nd Year (Yearly Retesting and Reassessment)	100% payment on completion of Phase -2
3	Review Audit – 3rd Year (Yearly Retesting and Reassessment)	100% payment on completion of Phase -3

Payment towards review audit charges for the year will be done at the completion of review audit every year.

Other Terms & Conditions

a. Firm should deploy at least 3-5 personnel having experience in formulating IT Security Policy and Procedures in addition to Project Manager for the project.

b. The rates quoted should be based on fixed cost and all inclusive i.e. inclusive of service tax, cess etc. The rates quoted should not be altered or changed due to escalation on account of any variation in taxes, levies, cost of services etc. The price quoted should be written in words as well as figures and in case of discrepancies between prices written in words and figures, the prices written in words shall be considered to be correct.

c. GIC will neither provide nor reimburse expenditure towards any type of accommodation, travel ticket, transport, lodging, boarding, etc.

d. TDS will be deducted at applicable rates, as per rules of the Government, while making payment.

e. The technical and commercial bids made by the firm should be valid for 120 days from date of submission.

f. GIC will not be responsible for any courier/postal delays. Also, the bids received in open condition or not complying with stipulated conditions will not be considered.

g. Any decision as to compliance of the terms and conditions of the tender document and rejection of tender document or any part thereof shall be at the sole discretion of GIC. Any decision of GIC in this regard shall be final and binding on the tenderer.

h. GIC has the right to re-issue the tender.

i. On being the successful tenderer, the tenderer shall enter into an agreement (including but not limited to bank guarantee and indemnity) with GIC in the form and manner to the satisfaction of GIC substantially on the lines of the terms and conditions of the tender.

j. The organizations already providing IT related service(s) to GIC are not eligible to participate in this tender.

Annexure I

SCOPE OF WORK

The scope of work will encompass the Information Technology and Information Systems at the head office of GIC at Mumbai, Primary Site IT infrastructure at Netmagic Data Center, Vikroli, Mumbai and DR site IT infrastructure at Netmagic DC at Chennai.

It will include all activities needed to facilitate GIC in preparing an information security plan and implement the security control measures as per IS/ISO/IEC 27001 : 2005.
The identified audit firm will have to assess the IT security risk associated with the following departments and determine the acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievements of organizational goals/objectives.

The departments under the scope of work will be:

Reinsurance Operations and Accounts
Investment Operations and Accounts
Finance
ITMG
HR & Administration
Office Services

The entire project will comprise of following 3 phases:

Phase No.	**Phase Description**
1	Information Security Audit – 1st Year
	IPv6 Audit
2	Review Audit – 2nd Year (Yearly Retesting and Reassessment)
3	Review Audit – 3rd Year (Yearly Retesting and Reassessment)

Scope of IT Infrastructure Audit.

Section 'A'

1.1. Current state assessment which shall include the following:
- 1.1.1. DC infrastructure and Network (Primary Site at Netmagic Data Center, Vikroli, Mumbai and DR site at Netmagic Data Center,Chennai)
- 1.1.2. LAN Infrastructure (GIC HO)
- 1.1.3. Applications - Existing & Proposed
- 1.1.4. Security Infrastructure
- 1.1.5. Security Incidences
- 1.1.6. Others

1.2. Risk Assessment, Identification of risks and Prioritization of Potential Risks/Threats of IT assets and develop Risk mitigation plans based on the security needs.

1.3. Identify security measures based on the threat and risks identified in the risk assessment and the obligation of the organization to comply with various government policies, laws and regulations etc. These security measures can be selected from international standards such as ISO 27001 comprising of physical security, Human resource Security, networks and systems etc. They can be in the form of Security Policies and procedures and implemented through people process and technology.

1.4. Gap analysis vis-à-vis International Best Practices and prevailing regulations.

1.5. Vulnerability Assessment / Penetration Test.

1.6. A Business Continuity Process needs to be implemented to counteract interruption to business activities and to protect critical processes from major failures and ensure their timely resumption to an acceptable level through a combination of preventive and recovery controls.

1.7. Develop Continuity and Disaster recovery plans for the same.

1.8. Preparation of the Statement of Applicability.

1.9. Preparation of Security Policy document.
Review existing IT Security Policy and Procedures to give adequate control over Information Systems assets and help manage IT risks effectively. Develop and document a comprehensive set of leading security policies and present the same to the Forum for approval. The vendor will carry out amendments as agreed in the forum and present the same again.

1.10. Training and awareness.

Section 'B'

Deliverables

The deliverables should include:

1. Current State Assessment Report.

2. Gap analysis report. This document should include details about the gaps in the current setup and ways to mitigate the same. It should provide information on the Hardware/Software that will be required to be put in place to get over security loopholes. Eg. Firewall, IDS etc. It should also throw light on the changes that need to be carried out in the Security infrastructure in view of the existing and proposed applications.

3. Penetration Test Report/ Vulnerability Assessment Report.

4. Risk Assessment Report.

5. Risk Treatment Plan.

6. Statement of Applicability.

7. Security Policy and procedures Document.

8. End User training Workshop.
9. Business Continuity Plan / Disaster Recovery Plan.

Any other necessary documentation for attaining the ISO 27001 Certification
The broad parameters, which are required to be reviewed by the Auditor, are as under:

Network and Security Audit

- Conducting Network Security Architecture Review of GIC's Network at Data Centers in Mumbai and Chennai.
- Review the applications, network, servers and services within an organization's environment and identify methods to enhance and improve on the system infrastructure and support.
- Technical Security Assessment.
  - Conducting vulnerability assessment / penetration testing.
- Review and evaluate/update the Security Policy & procedures document, providing guideline and management direction in implementing and enforcing company's information security goals/objectives with respect to Confidentiality, Integrity & Availability.
- Provide a confirmation that functioning of Data centers (Primary Site and DR site), GIC HO location mentioned above are in compliance with:
  - GIC's IT Security Policy
  - IRDA guidelines, any other legal requirements.

Network Security Architecture Review
The vendor shall do following activities:

• Understanding the traffic flow in the network, it includes:
- LAN
- Overseas Office connectivity

• Analyze the Network Security controls, which include study of logical locations of security components like firewall, IDS/IPS, proxy server, Antivirus server, Gateway level antivirus server, Citrix server, Email Servers, SAP servers, local servers etc.
• Study of incoming and outgoing traffic flow among application servers and database servers, and Active Directory from security point of view.
• Review of other applicable security aspects with respect to wired and wireless connectivity.
• Study and review of network architecture from disaster recovery point of view.
• Detailed report on findings with suggestions and recommendations on Network Security architecture

Configuration Audit of Network Devices (All locations mentioned in the scope of work)
The vendor shall do following activities:

- Study and analyze the network device's roles and configuration thorough configuration audit.
- Understand and evaluate the loopholes in the configuration, if any.
- Audit checklist for network devices.
- Configuration of all Network Equipments should be verified for any Security threats
- Report with suggestions and recommendations to rectify the above vulnerabilities.

Vulnerability Assessment (DC & DR)
The vendor shall do following activities:

- Port scanning of the servers, network devices and security devices/applications.
- Analysis and assessment of vulnerabilities.
- Network traffic observation for important and confidential information like username, password flowing in clear text.
- Perform a comprehensive scan of all IP address ranges in use to determine what vulnerabilities exist in the network devices and servers, and to review all responses to determine if any risks exist.
- Use vulnerability scanners to scan the critical/ network devices and servers to determine vulnerability exists.
- Search for back door traps in the Operating Systems.
- Router testing, Firewall testing
- Check for the known vulnerabilities in the Operating Systems, and applications like Browser, E-Mail, Web Server, and VPN etc.
- Use tools to perform a password scan to determine accounts that have passwords that are "easy" to crack.
- Test for the presence of unnecessary services/applications those are running on the network devices/servers/workstations.
- Prepare the Vulnerability Assessment Report consisting of an executive summary that expresses business risk and the technical nature of the risk and its seriousness, and a technical report that includes findings and mitigation strategies in full detail.
- Exploitation of vulnerabilities (with GIC's permission)
- Report with findings and recommendations.

Compliance of GIC's IT security policies procedures and provide recommendations

- Current IT infrastructure of GIC Re.
- Network and the devices in use
- Analyzing and Reviewing the activities performed in the network and operational procedures
- Reviewing role of existing Network Security controls
- \review role and impact of network services being used/ configured in the current network.
- Report submission for the above activities
- Review of security procedures including
  i. Incident response
  ii. Business continuity planning and disaster recovery
  iii. Configuration management, etc.

iv. Recommending Operational Procedure and policy for these processes.

Desktop Security Scanning.

The vendor shall do following activities on all desktops at GIC HO, each floor. (6 floors)

- Vulnerability scanning of desktop systems
- Observe, analyze and assess the operations being performed from desktop system
- Analyze the vulnerability scanning report
- Detailed report on findings with suggestions and recommendations.

Software License Compliance (DC & DR)

End-User Awareness Training

- Provide requisite training material for user training
- Conduct a session once every year for executives of GIC (at least 1 hour session)

Review Audit (Retesting and Reassessment) once per Year.

- Rechecking of gaps found during activities listed above and annual re-assessments.
- Vendor is required to retest and reassess after identified gaps have been remediated. This retesting may be required at any time during the contract period, but will be limited to 2 retests per identified gap.
- Reassessment exercises involving the activities listed above once every year or if required during any major infrastructure upgrade.

IPV6 Readiness (one time activity)

The bidder needs to do an audit of the readiness for IPV6 enablement. It must cover the following;

- Audit of the computers and networking equipments used in GIC to see if they are able to support 3 technology solutions {Dual Stack (Dual IP), Tunneling Techniques, Translation Techniques} devised by IETF (Internet Engineering Task Force), which will make IPv6 migration possible.
- Discover and understand the organizational objectives, scope and strategy where IPv6 is concerned.
- Compile information on the environment to ascertain IPv6 readiness of hardware, software and other operational components that forms IT infrastructure.
- Building on the information from the preceding stages, perform an in-depth analysis and determine IPv6 compliance of the infrastructure and application services in the existing environment.
- Recommend a framework, where major outputs in the form of reports and presentation will document the current state and offer recommendations that will help the organization advance towards the desired state of IPv6 capabilities. The report should bring out the following details but not limited to the below mentioned :
    - Cost-effective evaluation of IPv6 deployment and migration strategies without any impact on the production network.
    - Analysis and assessment of IPv4/v6 dual-stack device configurations.

- Summaries to understand the deployment process and present an approach supported by quantitative data concerning the impact of the migration.
- Determination of which network devices/hardware need software upgrades to support IPv6 capabilities.
- The planning service can also include analysis to predict the impact of the transition on mission critical application performance.

Annexure II

TENTATIVE LIST OF NETWORKING EQUIPMENTS & SERVERS

Categories	Sub-Categories	Current Solutions
Data Architecture		
	Corporate Databases	Oracle 10g, MS SQL Server
	Applications	SAP ECC 6, BI 7.0, EP7.0, PI 7.1, BOBJ, RiskLink 11.0 (Risk Management Solution), Document Management System (Newgen), Mailserver (Emergic Mailserv), Renova (Life Reinsurance Solution).
Platforms		
	Windows Servers (OS)	Win 2003, Win 2008
	Unix Servers (OS)	HP-UX
	Linux Servers (OS)	RHEL 5.0, RHEL 4.0
	Corporate Servers	HP Itanium (rx 3600, rx 2660), HP Xeon (DL 380, ML 370), HCL Xeon (GL 2700), Dell M910, Hp Proliant DL180G6
Enterprise Storage		
	Corporate Storage	HP EVA 4400, HP EVA 4100, EMC Clariion.
Network		
	Wide Area Networks	IPSec VPN, Site to Site and Citrix
	Voice Services	NA
Other Company Owned Equipment		
	Racks	5
	Network Routers/Switches	Cisco 1841, Cisco 4506, Cisco 2960, Cisco 1900
	Firewall	**Cisco ASA 5520 (nos. 6)**

LAN Component	Nos.
Edge Switches	16
Distribution Switches	10
Core Switches	2
Routers (Cisco 1941)	3
SAN Switches	2
Type of cabling	Structured CAT-5/6 and Backbone on Fiber.
Desktops	500 plus
Laptops	100

Details of Servers (Including Data Centre and DR site)		
Type of servers	**Operating System**	**No of Servers**
SAP Application Servers	RHEL	14
Email	Windows server 2008	7
e-Thru Application	RHEL	7
Citrix Server	Windows server 2008	1

DMS Servers	RHEL	4
RMS Server	Windows server 2008	1
NDS	Windows server 2008	1
Life –Re	Windows server 2008	1
Saprouter	Windows server 2008	1
Active Directory	Windows server 2008	2
Web Proxy server	RHEL	1

2. Details of Internet/Trusted Networks		
Type/Name	**Type of connectivity**	**Service Provider**
Internet	Broadband	
	Leased Line	10 Mbps Internet Leased Line.
	Leased Line	DC to GIC (20 mbps Point to point MPLS)
		DR - GIC (20 Mbps Point to point MPLS)
	Reuters	
	NDS	MPLS 2 x 64 kbps (Sify and Reliance links)

During the time of audit if there are additional equipments, they shall also be considered for audit purposes.

Annexure III

BIDDER'S INFORMATION

1. Name
2. Constitution and year of establishment
3. Registered Office/Corporate office/Mailing Address
4. Names & Addresses of the Partners if applicable
5. Contact Person(s):
6. Telephone, Fax, e-mail
7. Whether empanelled by CERT-In. (State the period of empanelment along with documentary proof)
8. Number of CISA/ CISSP Qualified persons who would be involved in the Audit work along with names and experience.
9. Number of CCNA/ CCNP Qualified Persons who would be involved in the Audit work along with the names and experience.
10. Number of BS7799 lead auditors / ISO 27001 ISMS Lead Auditors who would be involved in the Audit work along with the names and experience.
11. Number of years of experience in Information Security Audit. Furnish client list for projects handled related to Information Security. Briefly mention about a minimum of 3 Information Security related projects carried out (Include Insurance organizations, if any).
12. Describe Project Management methodology for the proposed Information Security Audit assignment, clearly indicating about the composition of various teams.
13. Describe Audit Methodology and Standards to be used for Information Security Audit.
14. Indicate Project Plan with milestones and the time frame of completion of different activities of the project.
15. List of Deliverables as per the 'Scope of Work'.
16. Details of Location and infrastructure of Security Operations Centre from where services such as external vulnerability analysis and problem response are managed.
17. Any other related information, not mentioned above, which the audit firm wish to furnish.
18. Details of organizations where IPv6 audit has been done by the vendor previously along with the scope involved.

19. Describe Project Plan with milestones and the time frame for completion of different activities to be performed for carrying out IPv6 audit.

20. List of Deliverables for IPv6 Audit.

DECLARATION

We hereby declare that the information submitted above is complete in all respects and true to the best of our knowledge. We understand that in case any discrepancy or inconsistency or incompleteness is found in the information submitted by us, our application is liable to be rejected.

Date: Authorised Signatory.

Note:

The Technical Bid shall include the detailed project plan corresponding to the deliverables as required by GIC Re for the Project. The project plan should indicate the milestones and time frame of completion of the different activities of the project. The audit firm is required to give details of the project management methodology, Audit Standards and methodology along with the quantum of resources to be deployed for the project, in the technical bid. Resources and support required from the Corporation should also be clearly defined.

Annexure IV

FORMAT OF CURRICULUM VITAE (CV)
(Separate sheets for each person to be Assigned to the project)

Position:

Name of Firm:

Name of Personnel:

Qualifications

Date of Birth:

Years with Firm:

Nationality:

Membership of Professional Societies:

Detailed Tasks Assigned (past 5 years):

(Giving an outline of person's experience and training most pertinent to task on assignment. Describe degree of responsibility held by the person on relevant previous assignments and give dates and locations)

Employment Record:
(Starting with present position, list in reverse order)

Qualifications: Technical and Academic with year of passing:

Annexure V

Format of Commercial Bid

Phase No.	Phase Description	Cost excluding taxes (Rs.)	Taxes (Rs.)	Total Cost with taxes (Rs.)
1	Information Security Audit – 1st Year			
	IPv6 Audit			
2	Review Audit – 2nd Year (Yearly Retesting and Reassessment)			
3	Review Audit – 3rd Year (Yearly Retesting and Reassessment)			
	Total			

The Commercial bid should be in the exact format as given above. Any deviation may lead to disqualification of the bidder.

Payment terms will be as follows:

100% against delivery and completion after the submission of deliverable and proper sign off at the end of each phase as listed above.

Payment towards review audit charges for the year will be done at the completion of review audit every year.

NOTE: It is expected that the firm will accept all the terms & conditions as stipulated by GIC. In case, some conditions are not acceptable or any additional conditions are stipulated, the same may be indicated here. The change in terms and conditions by the firm, if any, should also be mentioned in the technical bid.

Date:

Name of Authorised person

Designation

Signature

Company Seal