Pre-Bid Queries and Responses - Selection of Consultant for Independent External Information Security Audit & other related services

Bid Number: GEM/2026/B/7431894

Responses to the Pre-bid queries received upto 23.05.2026

Q.No	Queries	GIC Re Clarification / Response
1	This Bid provides for Trade Receivables Discounting System (TReDS) as Preferred mode of payment. For MSME sellers, payments may be processed through a TReDS exchange in which the Buyer is registered, subject to applicable policy and regulatory guidelines. Accordingly, sellers intending to avail payment through TReDS are required to be registered with at least one TReDS exchange in which the buyer is registered." In this regard, bidder requested to confirm how the payment will be processed for this contract. Further, we request you to kindly keep the payment terms and conditions simple and avoid making payment processing mandatory through the TReDS exchange platform, considering our earlier experience with the same.	Regular payment mode through bank after processing invoice submitted.
2	Please confirm do we need to submit the EMD. As per the law Micro & Small Enterprises (MSE) units and Start-ups* are exempted from payment of EMD and tender fee provided the Services they are offering are rendered by them. Exemption as stated above is not applicable for providing services, rendered by other companies. Bidder should submit supporting documents issued by competent Govt. bodies to become eligible for the above exemption.	Micro & Small Enterprises (MSEs) are exempted from paying Earnest Money Deposit (EMD) in government tenders. This exemption applies to MSEs registered under Udyam Registration or with NSIC for the goods produced or services provided subject to submission of relevant supporting documents
3	We understand that if security audits are conducted for the same organization for two separate years under a single Agreement / Purchase Order, the same will be considered as two separate instances of experience. Kindly confirm.	Security Audits conducted under Purchase order/contract with one organization will be considered as one instance only irrespective of number of years.
4	Kindly confirm whether ongoing projects will also be considered for eligibility and experience evaluation.	Only completed projects will be considered for experience.
5	The Bidder should have successfully completed same or similar category of services, where the value of contract/s is/are (a) not less than 80% for 1 order or (b) not less than 50% for 2 orders or (c) not less than 40% for 3 or more orders of the estimated Bid value, in at least one of the last three Financial Years before the Bid Opening Date to Any Central / State Govt Organization/PSU.	No query for any clarification.
6	Kindly clarify whether the Integrity Pact must be submitted at the time of bidding or after the empanelment; Do we need to submit it on stamp paper? If yes then what would be the value of stamp paper.	Kindly refer to Point 14 of Prequalification Criteria (PQC) of the RFP. Stamp duty applicable will be Rs 500/-
7	What is the scope of coverage for foreign locations?	Scope of coverage will be the same for all locations.
8	Are foreign offices (Dubai, London, etc.) fully in scope for VAPT or only selective systems?	All systems are full in scope; please refer to GIC Re Response Q.7
9	Web Application Audit Kindly provide the following details: 1.Total number of applications 2.Number of static pages 3.Number of dynamic pages 4.Number of input fields 5.Types of users 6.Roles of each user	1&2. Approx. count 20 mostly dynamic pages; 3-6. Details will be discussed with the selected bidder during the kickoff meeting.
10	Mobile Application Audit Kindly provide the following details: 1.Total platforms (iOS / Android / IPA) 2.Total number of roles 3.Number of screens 4.Total number of input fields	1. Approx. count 2; 2-4. Details will be discussed with the selected bidder during kickoff meeting.
11	Kindly provide the total number of web services and methods required to be covered under the audit scope.	Please refer to GIC Re's responses to Q.43 & Q.84
12	Kindly provide the total number of servers in scope.	Approx. count - 100
13	Kindly provide the total number of databases in scope.	Approx. count - 50
14	Kindly provide the total number of network devices (routers / switches / load balancers).	Approx. count - 160
15	Please provide the count of in-scope IT assets covered, along with details of the tentative infrastructure setup.	Please refer to GIC Re's responses to Q.9; Q.10; Q.12; Q.13;Q.14; Q.25 & Q.27
16	What is the approx. count of IPs, applications, users, security and network devices to be assessed?	Please refer to GIC Re's response to Q.15
17	Please clarify the count of internet-facing assets and internal assets (intranet apps, internal APIs, admin portals, middleware, batch jobs).	Please refer to GIC Re's response to Q.9
18	Confirm exact quantity of assets per quarter for quarterly VAPT.	Please refer to GIC Re's to response Q.15
19	Please provide the total number of web applications in scope, along with classification (critical/non-critical). Are APIs included in this scope, or will they be assessed separately?	Please refer to GIC Re's responses to Q.9 & Q.34
20	Kindly provide the total number of security devices (IPS / IDS / Firewalls).	Please refer to GIC Re's response to Q.21

Q.No	Queries	GIC Re Clarification / Response
21	Please provide the list of security tools in scope: DLP, EDR, Antivirus, SIEM, email security, etc.	SIEM/ SOAR (FortiNet); EDR (Sentinel One); PIM/ PAM (Arcon); DLP (Forcepoint); NGFW (FortiNet), MDM (Microsoft Intune) etc.
22	Kindly clarify the frequency of revalidation audit – whether it is required quarterly or once after completion of all four quarters.	Revalidation Audit shall be conducted quartely. The Audit process includes an initial scan, followed by a rescan for all audits conducted.
23	Kindly confirm whether all devices are accessible from one centralized location. Also confirm the audit location(s).	All the devices are accessible by GIC Re - HO.; Audit location - General Insurance Corporation of India, "Suraksha, 170 J Tata Road", Churchgate, Mumbai 400020
24	Kindly provide: • Total number of users / email accounts for phishing activity • Frequency of phishing audit (Biannual / Annual)	Phishing exercises shall be conducted internally by the corporation; the selected bidder shall assist in assessing the effectiveness of the exercise & email security controls. Selected bidder shall provide recommendations to enhance overall security posture.
25	Kindly provide the total number of endpoints (desktops / laptops).	Approx. count - 750
26	Kindly provide the total number of locations to be covered under architecture audit.	Please refer to section A in scope of work.
27	Kindly provide the total number of wireless devices in scope.	Access points (Approx. count -100); Biometric device(Approx. count -15); CCTV (Approx. count-30)
28	“Review remediation of previous audit findings” - Kindly provide the total count of previous audit findings that are required to be reviewed for remediation status.	Shall be discussed with selected bidder during the kickoff meeting
29	“IT General Controls (ITGC) Audit Report (including SAP ITGC) with key findings and remediation recommendations.” - Kindly provide: • Total number of applications to be covered under the ITGC Audit scope • Total number of SAP modules implemented and in scope for review	ITGC Audit scope (Approx. Count - 5); SAP Module (Approx. Count - 10)
30	“Review of Security Policy, Standards & Procedures / Other Documents (Annually)” - Kindly clarify whether the scope is limited to review and recommendation of changes in policy/procedure documents only, or whether validation of implementation and compliance with the policies/procedures is also required.	The scope includes review and recommendation of changes to policy & procedure documents, along with validation of implementation and compliance with the policies & procedures
31	“Cybersecurity Awareness, Training & Phishing Simulation” - Kindly confirm: • Whether awareness/training sessions are required onsite at GIC Re premises or whether remote/virtual sessions would also be acceptable • Expected duration of each session • Expected number of phishing campaigns per year • Target user count per campaign	Cybersecurity awareness/training sessions are required to be conducted onsite at GIC Re premises; duration shall be discussed with the selected bidder during the kickoff meeting. Regarding Phishing campaign, please refer to Q.24
32	“Cloud Security Posture Management (CSPM)” - Kindly confirm: • Whether GIC Re is using private cloud or public cloud infrastructure • In case of public cloud usage, kindly provide cloud service provider details and hosting locations • Whether onsite visits to cloud service provider locations would be required as part of the audit	• Hybrid, private and Public both; • M365, India; • Please refer to section A in scope of work.
33	“AI / ML System Security Audit” Kindly confirm whether GIC Re currently uses any AI/ML based systems/applications. If yes, kindly provide the number of AI/ML models deployed or under development.	The Corporation is in the process of procuring GPUs; Details regarding the deployed AI/ML Models shall be shared with selected bidder as and when required.
34	“API & Integration Security” Kindly provide the total number of APIs falling under the audit scope, including both internal and external APIs.	currently, the corporation holds no APIs; In the future, any inclusion into the existing system shall be shared with selected bidder as and when required.
35	“ISO/IEC 27001:2022 Compliance and Information Security Assessment” Kindly confirm whether GIC Re currently holds a valid ISO/IEC 27001:2022 certification. If yes, kindly provide: • Current certification version • Certificate validity / expiry date Also clarify the detailed scope for ISO/IEC 27001:2022 assessment, including the locations/sites required to be covered for the gap analysis activity.	Currently Corporation does not hold the certification, as and when required the same shall be initimated to the selected bidder.
36	“Advanced Audit Activities” The RFP mentions that activities covered under Section B of the Scope of Work may be undertaken upon specific request from GIC Re, and that GIC Re reserves the right to change the frequency of such activities. Since the commercial bid would be submitted considering one instance of audit activity, kindly clarify whether a separate Work Order / Purchase Order would be issued in case the frequency exceeds one instance. Additionally, kindly confirm the audit location for each activity mentioned in the scope.	Yes, a separate Work order/ Purchase Order as per the accepted bid shall be issused for any increase in frequency; The audit location will be at General Insurance Corporation of India, "Suraksha, 170 J Tata Road", Churchgate, Mumbai 400020

Q.No	Queries	GIC Re Clarification / Response
37	"Re-audit" - Kindly confirm the expectations from the auditors with respect to vulnerability closure and remediation support. Are the auditors required to perform continuous follow-up and validation activities until all identified vulnerabilities are fully closed?	The selected bidder shall perform revalidation & Follow up until all identified vulnerabilities are fully closed.
38	How many revalidation rounds are expected if certain vulnerabilities remain unresolved after the first revalidation round?	Please refer GIC Re's response to Q.37
39	"Re-audit" - Kindly provide the frequency of audit for each activity mentioned in the Scope of Work.	The re-audit shall be conducted for all initial audits performed by the auditor.
40	Do you have SBOM, CBOM, and AIBOM prepared and available?	Basic SBOM and CBOM available.
41	Kindly confirm whether source code review is included within the scope.	Souce code review and security checks as per regulatory requirement for in-house developments shall be included in the scope
42	Is source code review required, or only black-box/grey-box testing?	Please refer GIC Re's response to Q.41; Only black-box/grey-box/white-box testing shall be conducted as per industry standard.
43	Should audit benchmark against Industry standards or organization-specific policies?	The auditor shall follow audit benchmarks aligned with industry standards & regulatory specifications.
44	What is the approved testing window (business hours/non-business hours)?	Only during business hours.
45	Please confirm whether both authenticated and unauthenticated vulnerability scans are required for servers/endpoints, and whether privileged credentials will be provided.	Details will be discussed with the selected bidder during the kickoff meeting.
46	Please confirm whether third-party hosted/SaaS assets (e.g., Akamai, Office 365, other cloud services) are in scope for VAPT and what access will be provided.	No
47	"Network Infrastructure Security and Resilience Assessment" - Should the assessment include identification only OR detailed root cause analysis and remediation guidance?	The assessment includes identification and remediation guidance.
48	"Network Infrastructure Security and Resilience Assessment" - Will scope (number of devices/locations) remain fixed, or may it change during the engagement?	The enhancement in scope is subject to change in the event of any upgradation/Modification to the corporation's IT enviroment or as per regulatory guidelines.
49	Please share network diagrams (LAN/WAN/DMZ), IP range list, segmentation details, and list of security devices (FW/IDS/IPS/WAF/VPN/Proxy) to enable accurate scoping.	Please refer to GIC Re's Responses to Q.21 & Q.147
50	Please confirm whether device jailbreak/rooted testing is permitted and whether test devices will be provided by GIC Re or bidder.	No
51	Please clarify expected coverage for endpoints (sample-based vs full estate), and whether EDR-managed endpoints are in scope for scanning.	All EDR-managed endpoints are in scope for scanning; full estate of endpoints shall be covered.
52	Please confirm whether automated discovery tools are available and whether bidder can run scans to validate asset inventory completeness.	Shall be discussed with the selected bidder during the kickoff meeting.
53	"Information Systems (IS) Assurance Audit (Annually)" - Please confirm the total number of systems/applications in scope.	Regarding ITGC Scope, please refer to GIC Re's response to Q.29
54	Please provide the total number of policies, procedures, standards, SOPs in scope Are there any additional documents beyond the list mentioned?	IS Policy, IS Procedure (includes multiple sub-policies), & Other policies related to Information Cyber Security currently in use by the corporation for regulatory compliance.
55	"Review of Security Policy, Standards & Procedures/ other Documents (Annually)" - Kindly confirm against which standards shall the mapping be done.	Please refer to GIC Re's Response to Q.43
56	"Review of Security Policy, Standards & Procedures/ other Documents (Annually)" - Kindly confirm if drafting a new policy or updating an existing policy is in scope. Also if the templates shall be provided by GIC Re.	Yes, drafting new policies & updating existing policies are within scope.
57	"Regulatory Compliances" - Kindly confirm all the regulations applicable and mandatory for GIC Re.	As listed under scope of work, section 6 (Regulatory Compliance) & shall be discussed with the selected bidder during the kickoff meeting
58	"Regulatory Compliances" - Does “assist in implementing compliance” mean Advisory only or Hands-on implementation (policy drafting, control implementation, tool configuration)?	Please refer to GIC Re's Response to Q.30
59	"Regulatory Compliances" - Kindly confirm the frequency of assessments that are mentioned in the clause.	The selected bidder shall provide assistance as & when required by the corporation to ensure regulatory compliance.
60	"Regulatory Compliances" - Kindly confirm the expected turnaround time for responding to regulatory queries?	Depending on the timeline prescribed by the regulator.

Q.No	Queries	GIC Re Clarification / Response
61	"Asset Management & Data Protection: (Annually)" - What is the total number of IT assets across: Hardware, software, virtual assets, cloud resources, and data repositories?	Please refer to GIC Re's response to Q.15
62	"Asset Management & Data Protection: (Annually)" - Are third-party, cloud-hosted, and shadow IT assets included in scope?	No
63	"Asset Management & Data Protection: (Annually)" - Should audit follow sample-based approach or full validation across assets?	Sample-based approach may be adopted & it can be extended to full validation depending on the nature/criticality of the asset.
64	"Asset Management & Data Protection: (Annually)" - Who will define the sampling criteria and size?	Shall be discussed with the selected bidder during the kickoff meeting.
65	"Asset Management & Data Protection: (Annually)" - Kindly confirm the applicable data protection, privacy, and regulatory requirements to GIC Re.	DPDP Act, 2023 along with regulatory compliance requirements listed under section 6 of scope of work.
66	"Identity & Access Management (IAM): (Annually)" - Which systems are in scope for IAM review 1. AD, SAP, enterprise applications, databases, network devices, cloud platforms? 2. Are cloud-based identity systems (e.g., Azure AD/Entra ID, IAM in AWS) included?	1.AD, M365, network devices. 2.No
67	Please confirm whether the engagement requires mandatory onsite presence, or if it can be executed in a hybrid (onsite + remote) model.	Execution may be carried out in a hybrid model (onsite & remote), subject to accessibility of network & applications.
68	Please confirm whether the client will provide scanning tools/ licenses (if required) or bidder shall provision all tooling.	Bidder shall make provision all required audit tools.
69	"Config Audit of DLP/EDR/Security Apps (Annual)" - Please list in-scope tools (DLP, EDR, AV, WAF, IDS/IPS, PAM, CASB, MDM etc.) and confirm whether SaaS security configurations (e.g., M365 security) are included.	Please refer to GIC Re's response to Q.21; Yes, SaaS security configurations review are included within the scope.
70	"Asset Management & Data Protection: (Annually)" - Please clarify whether privacy requirements (DPDPA) mapping is expected here OR is it limited to cybersecurity controls (classification, retention, encryption).	Scope shall be limited to cybersecurity controls
71	Web Application Testing 1.Total Number of Applications 2.Number of applications for black box testing 3.Number of applications for grey box testing (DAST) 4.Approx. number of dynamic and static pages in each applications? 5.Number of user roles defined in an application which needs to be tested (average)	Please refer to GIC Re's response to Q.9
72	Mobile Application Security Testing 1.Total Number of Applications 2.Count and Platform of Application (SAP/Android / iOS / Windows / Blackberry) 3.Nature of Application (Native / Hybrid) 4.Approx. number of dynamic and static functionalities in the application? 5.Black box (unauthenticated) or Grey box (authenticated) scan to be performed? 6.Number of different user 'levels' and is testing required for every user level?	Please refer to GIC Re's response to Q.10
73	API Testing 1.Total Number of APIs 2.Type of APIs (SOAP / REST) 3.Black box (unauthenticated) or Grey box (authenticated) scan to be performed? 4.Number of different user 'levels' and is testing required for every user level?	Please refer to GIC Re's response to Q.34
74	Thick Client Testing 1.Will the application executable and installation package be provided for local testing? 2.Should the assessment include backend/API communication and local storage (e.g., files, registry)? 3.How many thick client applications/versions need to be tested?	Thick client application testing shall depend on GIC Re's procuement of any software in the future, the audit methodolgy/process shall be discussed with seected bidder during the kickoff meeting.
75	Network vulnerability assessment and penetration testing 1.Total count of External Ips including Database, Operating System, Web Server, Docker and Other Components 2.Total count of Internal Ips including Database, Operating System, Web Server, Docker and Other Components	Please refer to GIC Re's response to Q.15
76	Source Code Review 1.Number of applications 2.Number of lines of code to be reviewed per application	At present, no estimates can be provided regarding number of applications. Also please refer to GIC Re's response to Q.41 & Q.42
77	Cloud Security Assessment 1.Number of cloud platform and subscriptions to be reviewed as part of the scope 2.Number of SAAS application to be reviewed under the scope	Approx. count - 5

Q.No	Queries	GIC Re Clarification / Response
78	Configuration Audit 1.Count of Devices along with Asset type (Server/Network Device/ Access Point)	Please refer to GIC Re's response to Q.15
79	Network Architecture Review 1.No of locations to be covered 2.Network Architecture Diagram present (HLD and LLD)	All locations mentioned under section A of Scope of work are included; both HLD & LLD are available.
80	Wi-Fi Testing 1.List the number of WiFi Access points/routers/device 2.Details on number of locations to be covered	1.Please refer to GIC Re's response to Q.15; 2.IT systems located at sites other than GIC Re HO shall be tested via remote connection. GIC Re will facilitate the selected bidder in establishing the remote connection.
81	Red Team Assessment 1.Internal / External / Both 2.If Phishing Campaign is part of scope.If yes,How many Campaigns to be considered 3.If Physical Security Assessment is part of scope 4.Are there specific threat actors, attack scenarios, or risks you would like us to simulate? 5.Are there any particular breach scenarios you want us to prioritize during the Red Teaming (e.g., insider compromise, ransomware attack, or data theft)?	Please refer to GIC Re's response to Q.24
82	Will the testing be performed onsite or remote? If onsite, mention location.	Please refer to GIC Re's response to Q.67
83	Will revalidation be performed? If yes, how many cycles of revalidation are required?	Please refer to GIC Re's Responses to Q.22 & Q.37.
84	What is scope of Web Application Security Audit?	Assessment shall include OWASP Top 10 & identification of all known vulnerabilities in applications, based on internationally recognized standards and frameworks.
85	Vulnerable Assessment and Penetration testing: 1.Share the indicative asset inventory (IP ranges, applications, APIs, mobile apps) for effort estimation. 2.Provide an approximate count of IPs, servers, databases, endpoints, and security devices expected to be covered per quarter? 3.How is the testing expected to be conducted (black-box/grey-box/white-box)? Will access credentials be provided where required? 4.Are there any constraints around exploitation, especially for production environments or DoS scenarios? 5.What is the expected timeline per quarterly cycle and overlap between assessments? 6.Is there a cap on number of applications/APIs/assets per quarter for commercial purposes?	1 & 2. Please refer to GIC Re's response to Q.15; 3.Please refer to GIC Re's response to Q.42 & Yes, Credential shall be provided. 4 & 5 - shall be discussed with the selected bidder during kickoff meeting. 6. There is no cap on number of applications/API/Assets per quarter
86	Network Infrastructure Security & Resilience Assessment: 1.Share a high-level count and types of network devices in scope (firewalls, routers, switches, VPNs, IDS/IPS, WAF, etc.)? 2.Will network diagrams and configuration backups be made available for review? 3.How broad is the coverage expected across DC, DR, HO, and international locations? 4.Should we include DR/failover validation activities, or is the scope limited to assessment only? 5.Are there any devices or components that would require coordination with OEMs/vendors? 6.Confirm whether there is any standard checklist/template to be followed, or should we proceed with our own methodology aligned to industry practices?	1.Please refer to GIC Re's response to Q.15; 2.yes, Network diagrams & configuration backups shall be made available for review. 3. The expected audit coverage shall align with industry best practices and ensure full compliance with all applicable regulatory provisions relating to information security, cyber security, and digital personal data protection. 4.the scope shall be limited to assessment only 5.Yes, but coordination shall be carried out internally by GIC Re. 6.Audit methodology shall be discussed with the selected bidder during the kickoff meeting
87	Configuration Audit of DLP, EDR and other Security Tools: 1.Share the list of security tools in use (DLP, EDR, AV, SIEM, etc.) along with their deployment coverage? Roughly how many endpoints and servers are integrated with these tools? 2.Will we be given access to consoles, configurations, and logs for the assessment? 3.Is the expectation limited to a configuration review, or should we also evaluate effectiveness using simulations/use cases?	1.Please refer to GIC Re's Response to Q.21; 2.Yes; 3.the scope shall be limited to configuration audit.

Q.No	Queries	GIC Re Clarification / Response
88	IS Assurance Audit: 1.Kindly share the scope boundary (systems, business processes, applications like SAP) covered under ITGC and IS audit. 2.What is the sample size expectation for control testing (users, transactions, logs)? 3.Will previous audit reports and ATRs be available for reference and validation? 4.Are we required to strictly follow IRDAI reporting formats/annexures?	1. Regarding the Scope of ITGC, please refer to GIC Re's response to Q.29 & IS Audit, the scope covers entire IT infrastructure/environment of GIC Re; 2.shall be discussed with the selected bidder during the kickoff meeting; 3.Yes; 4.Yes, in accordance with IRDAI Annexure III & V.
89	Security Policy & Document Review: 1.Could you indicate the approximate number of policies, SOPs, and procedures to be reviewed? 2.Is the work expected to be limited to gap assessment, or should we also support redrafting and approvals? 3.Will this involve workshops/discussions with stakeholders during the review process? 4.Are there any standard templates or regulatory mappings (IRDAI/CERT-In) that need to be followed?	1.Please refer to GIC Re's response to Q.54; 2.Please refer to GIC Re's response to Q.30; 3.Yes; 4.Yes, in accordance with IRDAI ICS 2026 & all applicable regulatory guidelines for the corporation.
90	Regulatory Compliance Support: 1.Kindly confirm the list of applicable regulations prioritized for compliance (IRDAI, CERT-In, SEBI CSCRF, MeitY, etc.). 2.What is the expected level of involvement in compliance (advisory vs implementation support)? 3.How often are regulatory audits/third-party assessments expected during the contract period? 4.Should effort include response to partner/regulator questionnaires on an ongoing basis?	1.Shall be discussed with the selected bidder during the kickoff meeting ; 2.Please refer to GIC Re's response to Q.30; 3.As & When the need arises; 4.Yes.
91	Asset Management, Data Protection & IAM: 1.Kindly share the estimated number of assets, users, privileged accounts, and data repositories. 2.Are there existing asset inventories and data classification standards already in place? 3.Which IAM/PAM tools or platforms are currently deployed? 4.Should the scope include a detailed validation of data privacy controls (PII handling, encryption, retention, etc.)?	1. Users roughly 800-900; for assets please refer to GIC Re's Response to Q.15; priviledge accounts - approx. count 30; DB - please refer to GIC Re's Response to Q.13. 2.Yes; 3.Please refer to GIC Re's Response to Q.21; 4.Yes.
92	Logging, Monitoring & SOC: 1.Kindly provide details of SIEM/SOC setup (tools, log sources, coverage). 2.What is the number of integrated systems/log sources to be reviewed? 3.Are use-case effectiveness, alert tuning, and incident simulations expected? 4.Is there a requirement for 24x7 monitoring review vs periodic assessment only? 5.For logging, monitoring, and SOC assessment, does GIC Re have existing evaluation checklists/use-case review templates, or should the bidder perform assessment using its own methodology?	1.Please refer to GIC Re's response to Q.21; 2. 150 log sources roughly, integration details will be shared with selected bidder (not less than 10) 3.No; 4.Periodic assessment only; 5.Shall be discussed with the selected bidder during the kickoff meeting.
93	Cybersecurity Awareness & Phishing Simulation: 1.Kindly confirm the total number of employees/users to be covered for awareness sessions. 2.Will user segmentation (It staff, management, board) be required? 3.What is the expected frequency and scale of phishing campaigns? 4.Should training content development and LMS integration be included? 5.Can GIC confirm that “5 sessions per year” refers strictly to training/awareness sessions only?	1.Shall be discussed with the selected bidder during the kickoff meeting; 2.Yes; 3.Please refer to GIC Re's response to Q.24; 4.Only training content development is included; 5.Yes, for training/awareness session only.
94	Cloud Security Posture Management (CSPM): 1.Kindly share cloud environments (AWS/Azure/GCP) and number of accounts/subscriptions. 2.Is tool-based CSPM expected or manual assessment sufficient?	1. Approx. count - 5; 2. Shall be discussed with the selected bidder during the kickoff meeting
95	"AI/ML Security" - Kindly confirm if AI/ML systems currently exist, and provide details of pipelines/models in scope.	Please refer to GIC Re's response to Q.33
96	"API & Integration Security" - Provide number of APIs/endpoints and integrations along with documentation availability.	Please refer to GIC Re's response to Q.34 & Q.85

Q.No	Queries	GIC Re Clarification / Response
97	ISO 27001:2022: 1.Is the scope limited to gap assessment or end-to-end certification support? 2.Are existing ISMS documents and prior certifications available?	1.Shall be discussed with the selected bidder during the kickoff meeting; 2.Please refer to GIC Re's response to Q.35.
98	Re-Audit: 1.What is the expected frequency and scope of re-audits across activities? 2.Should all findings be retested or only critical/high-risk items?	Please refer to GIC Re's Responses to Q.22 & Q.37.
99	Kindly confirm the total number of assets per category to avoid scope creep.	Please refer to GIC Re's responses to Q.9; Q.10; Q.12; Q.13;Q.14; Q.25 & Q.27
100	Will on-site visits be mandatory for all locations or primarily remote?	please refer to GIC Re's response to Q.67
101	Can you define SLAs for report submission (currently within 30 days) and any penalties?	Please refer to clause 27 (Page 25) under Agreement.
102	Are travel costs for site visits to be reimbursed or included in bid price?	The bidder shall be deemed to have included all costs and expenses necessary for the performance of the work including site visits in their bid. Under no circumstances GIC Re will be liable to pay or reimburse the Bidder for any travel expenses, subsistence costs, or other out-of-pocket disbursements.
103	Is there a defined annual calendar or expected workload distribution across 2 years?	Shall be discussed with the selected bidder during the kickoff meeting. Please refer to "others" section in the Scope of Work.
104	For DC (Mhape) and DR (Hyderabad), in case of location change before 2028, will scope automatically extend to the new sites?	Yes
105	Location of the Engagement: Does this activity need to be conducted onsite or remote? Further, kindly confirm if DC /DR needs to be visited. If yes, please let us know the locations of the sites	Please refer to GIC Re's response to Q.67; No
106	Configuration Audit of DLP, EDR and Other Security Applications: 1.Please confirm whether the assessment is expected to cover DC, DR, cloud, branch offices, remote endpoints, and third-party hosted environments. 2.Kindly confirm whether configuration reviews are expected against OEM hardening guidelines, CIS Benchmarks, IRDAI Guidelines, CERT-In advisories, or any internal baselines defined by GIC Re.	1. Yes; 2.Configuration review shall be conducted against OEM hardening guidelines, CIS Benchmarks, IRDAI Guidelines, & CERT-In advisories.
107	"IS Assurance Audit" - Kindly confirm the total number of applications, databases, SAP modules, operating systems, and infrastructure components that will be covered under the IS Assurance and ITGC audit.	For ITGC Audit, Please refer to GIC Re's response to Q.29; For IS Assurance Audit, please refer to GIC Re's Response to Q.88
108	"IT General Controls (ITGC) Audit including SAP ITGC" - Kindly clarify whether the ITGC audit (including SAP ITGC) is expected to be conducted as a separate assessment in addition to the IRDAI IS Assurance Audit, or whether ITGC review forms part of the overall IS Assurance Audit scope.	ITGC Audit shall be conducted as a separate assessment and the cost of such audit is deemed to have included in the Bid.
109	"Review of Security Policy, Standards & Procedures / Other Documents" - Kindly confirm the approximate total number of policies, standards, SOPs, procedures, baselines, and governance documents expected to be reviewed and updated under this engagement.	Please refer to GIC Re's response to Q.54
110	"Regulatory Compliances" - Please clarify whether the selected bidder is expected to perform independent compliance assessments only or also support implementation and ongoing compliance tracking activities.	Please refer to GIC Re's response to Q.30
111	"Regulatory Compliances – Certificates & Compliance Support" - Kindly clarify the specific types of certificates/reports expected from the selected bidder, the applicable regulatory or statutory requirements under which they are to be issued, and the detailed scope, activities, and deliverables expected as part of issuance of each certificate.	The selected bidder shall provide certificates/reports as may be required to submitted to regulatory authorities, Ministry etc. These shall include report/certificates required to be submitted to agencies/ authorities for obtaining certifications.
112	"Other Information Security Controls" - Kindly confirm the list of in-scope applications, systems, and business processes for which asset management, IAM, logging, monitoring, and security operations assessments are required to be performed.	Please refer to GIC Re's response to Q.15
113	"Asset Management & Data Protection" - Kindly confirm the scope of the asset completeness check, including the source systems/tools to be considered for validation. Further, clarify whether the review is limited to assets associated with in-scope applications only or covers all organizational assets across the enterprise.	Please refer to GIC Re's response to Q.15

Q.No	Queries	GIC Re Clarification / Response
114	"Logging, Monitoring & Security Operations" - Kindly confirm whether SIEM use case review, including assessment of alert logic, correlation rules, tuning, and coverage effectiveness, is part of the logging, monitoring, and security operations review scope.	No
115	"Infrastructure & Network Security Assessment" - Kindly confirm the approximate count of servers, network devices, firewalls, WAFs, VPNs, and security devices in scope.	Please refer to GIC Re's response to Q.15
116	"VAPT Scope" - Please confirm the approximate count of web applications, APIs, mobile applications, and external IPs in scope for quarterly VAPT.	Please refer to GIC Re's response to Q.15
117	"Remote Testing Requirement" - Kindly confirm whether all assessments are to be performed remotely from GIC Re HO Mumbai or if onsite visits will also be required.	Please refer to GIC Re's response to Q.67
118	"Configuration Audit" - Please confirm whether configuration audit of OS, databases, middleware, and web/application servers is also required.	Yes
119	"Controlled Exploitation" - Kindly confirm whether controlled exploitation of vulnerabilities in production is permitted with prior approval.	Shall be discussed with the selected bidder during the kickoff meeting.
120	"Application VAPT" - Please confirm whether authenticated testing credentials with multiple user roles will be provided for web and mobile applications.	Yes
121	"Mobile Application Security Assessment" - Kindly confirm the count of Android and iOS mobile applications in scope.	Please refer to GIC Re's response to Q.10
122	"Email Security Assessment" - Please confirm whether phishing simulation activities are also included as part of email security review.	Please refer to GIC Re's response to Q.24
123	"Network Infrastructure Security and Resilience Assessment" - Kindly confirm the approximate count of network devices and links to be covered under resilience assessment.	Please refer to GIC Re's response to Q.15
124	"Configuration Audit of DLP, EDR & Security Applications" - Please confirm the list and count of security tools/applications to be reviewed under this activity.	Please refer to GIC Re's response to Q.21
125	"IS Assurance Audit" - Kindly confirm whether SAP ITGC review is limited to application controls or also includes OS/DB level controls.	Limited to application controls
126	"Review of Security Policies & SOPs" - Please confirm the approximate number of policies, standards, SOPs, and procedures to be reviewed.	Please refer to GIC Re's response to Q.54
127	"Regulatory Compliance Support" - Kindly confirm whether support for regulatory audits and questionnaires is expected on unlimited occasions during the engagement period.	Please refer to GIC Re's response to Q.59
128	"Asset Management & Data Protection" - Please confirm whether data discovery and data flow review are also part of the assessment.	No
129	"Identity & Access Management" - Kindly confirm whether Privileged Access Management (PAM) solution review is included in scope.	Yes
130	"Logging, Monitoring & Security Operations" - Please confirm whether SOC/SIEM rule review and use-case validation are expected as part of the assessment.	Please refer to GIC Re's response to Q.92
131	"Cybersecurity Awareness & Phishing Simulation" - Kindly confirm the expected number of phishing simulation campaigns and targeted users during the engagement period.	Please refer to GIC Re's response to Q.24
132	"Cloud Security Posture Management" - Please confirm whether cloud assessment activities will be initiated only on specific request basis.	Yes

Q.No	Queries	GIC Re Clarification / Response
133	"API & Integration Security" - Kindly confirm whether third-party APIs and integrations are also included in the assessment scope.	Yes
134	"Re-Audit" - Kindly confirm the number of revalidation/re-audit rounds included during the engagement period.	Please refer to GIC Re's responses to Q.22 & Q.37.
135	"Audit Reports" - Please confirm whether separate reports are required location-wise, application-wise, and activity-wise.	Yes
136	"Report Format" - Kindly confirm whether editable reports in Word/Excel format are mandatory along with signed PDF copies.	Yes
137	"Deliverable Submission Timeline" - Please confirm whether the 30-day timeline for deliverables is applicable from completion of audit activity or from quarter end.	Yes, this shall further be discussed with selected bidder.
138	"New Applications / APIs" - Please confirm whether VAPT for newly deployed applications/APIs during the engagement period will be at no additional cost.	Yes, shall be at no additional cost.
139	"POC Support" - Kindly confirm whether dedicated SPOCs will be assigned by GIC Re for coordination of each assessment activity.	Yes
140	Could you please share the complete inventory of assets that fall under the scope? This would include IP ranges, applications, APIs, endpoints, mobile applications, Security Devices, and cloud environments.	Please refer to GIC Re's response to Q.15
141	In case new locations or systems are added during the contract period, how will these be handled from a commercial perspective?	At present, no additional locations are envisaged in the near future. However, any further locations or systems that do not constitute a material change in the scope of work shall be covered at no extra cost.
142	Will the VAPT activities be conducted on production systems, UAT environments, or both?	Shall be discussed with the selected bidder during the kickoff meeting.
143	"Access Requirements" - Should the assessment be carried out using authenticated scans, unauthenticated scans, or a combination of both?	Shall be discussed with the selected bidder during the kickoff meeting.
144	Apart from the 30-day report submission timeline, are there any defined timelines or SLAs for different stages of the engagement? Are there any penalties or liquidated damages applicable in case of delays in deliverables?	Regarding defined timelines or SLAs for different stages of the engagement, the same can be discussed with the selected bidder during the kickoff meeting. Regarding penalties or liquidated damages applicable in case of delays in deliverables - Please refer to GIC Re's response to Q.101
145	Are there any specific time windows or blackout periods during which testing activities should be avoided?	Shall be discussed with the selected bidder during the kickoff meeting.
146	Could you provide details of the security tools currently present in the network for configuration audit (for example: DLP, EDR, SIEM, email security solutions, etc.)?	Please refer to GIC Re's response to Q.21
147	"Access to Architecture" - Will relevant documentation such as network diagrams, system architecture, and configuration details be made available?	Yes, Shall be made available to the selected bidder.
148	"Re-Audit Scope" - How many re-audit or validation cycles are expected during the contract period?	Please refer to GIC Re's responses to Q.22 & Q.37.
149	Approximately how many new applications or APIs are expected to be tested annually under the “no additional cost” clause?	At present, no estimates can be provided regarding number of new applications/APIs to be tested under "no additional cost". Also please refert to GIC Re's response to Q.34, Q85 & Q.170
150	How many onsite visits are anticipated, and will travel and accommodation costs be covered by the client?	Please refer to GIC Re's response to Q.18
151	Could you please clarify the payment structure (e.g., quarterly, milestone-based, or annual payments)?	Please refer to clause 22 (Page 21) under Agreement.
152	"Tool Restrictions" - Are there any restrictions or guidelines regarding the use of commercial or open-source tools during the assessment?	Please refer to clause 7.2 (Page 14) under Agreement; All tools and software used by selected bidder for audit purposes must be genuine and licensed.
153	For overseas offices (Dubai, Kuala Lumpur, London), will audits be remote only or require onsite presence?.	Remote only.

Q.No	Queries	GIC Re Clarification / Response
154	Scope & Coverage: 1.Confirm number of locations, foreign offices, DC, DR to be covered. Any expected onsite visits? 2.Provide inventory count: servers, endpoints, network devices, applications, APIs, mobile apps. 3.Will secure remote connectivity be provided for all locations?	1.Please refer to section A in scope of work; 2.Please refer to GIC Re's response to Q.15; 3.Please refer to GIC Re's response to Q.80.
155	VAPT (Quarterly): 1.Total IP ranges, servers, devices in scope? Any exclusions? 2.Share network diagrams (LAN/WAN/DMZ, firewalls, IDS/IPS, VPN). 3.Is controlled exploitation permitted? Any restrictions? 4.Confirm quarterly schedule and expected timelines per cycle. (Frequency)	1.Please refer to GIC Re's response to Q.15; 2.Shall be provided to the selected bidder; 3.Shall be discussed with the selected bidder during the kickoff meeting; 4.Please refer to GIC Re's response to Q.103.
156	Threat & Vulnerability Assessment: 1.Threat Coverage - Any specific threat scenarios to prioritize (DoS, insider threat)? 2.Any mandated tools or methodology (CERT-In, OSSTMM)?	1.Shall be discussed with the selected bidder during the kickoff meeting; 2.Please refer to GIC Re's response to Q.152
157	Web Application Testing: 1.Applications - Number of web apps, environments (Prod/UAT), authentication type? 2.Complexity - Are apps transactional, API-heavy, or legacy? 3.Standards - Confirm OWASP/ASVS compliance level required.	1.Please refer to GIC Re's response to Q.9; 2. shall be discussed with the selected bidder during the kickoff meeting; 3.Please refer to GIC Re's response to Q.84.
158	Mobile App Security: 1.Number of Android/iOS apps? 2.Will APK/IPA or source code be shared? 3.Are backend APIs included in mobile scope?	1. Approx Count - 2; 2&3. Shall be discussed with the selected bidder during the kickoff meeting.
159	"Phishing Analysis" - Volume of phishing simulations or incidents to review?	Please refer to GIC Re's response to Q.24
160	Number of network devices (firewalls, routers, switches)?	Please refer to GIC Re's response to Q.15
161	List of tools (DLP, EDR, AV, SIEM)?	Please refer to GIC Re's response to Q.21
162	% of endpoints covered by these tools?	100%
163	IS Assurance Audit: 1.Coverage of ITGC, SAP controls, governance? 2.Any additional audit frameworks beyond IRDAI/CERT-In?	Please refer to GIC Re's responses to Q.29 & 88.
164	Policy & Document Review: 1.Number of policies/procedures to review/revise? 2.Expectation: review vs full redrafting?	Please refer to GIC Re's responses to Q.30 & 54.
165	Regulatory Compliance Support: 1.Frameworks - Confirm applicable standards (IRDAI, SEBI, CERT-In, MeitY). 2.Certifications - Any support required for certifications or audits? 3.Third-Party Queries - Expected volume of audit/partner queries?	1.Please refer to GIC Re's response to Q.88, Q.89 & Q.90; 2.Please refet to GIC Re's response to Q.35 & Q.102; 3.Please refer to GIC Re's response to Q.59.
166	Cyber Awareness & Training: 1.Number of users and sessions (5/year specified)? 2.Phishing Simulation - Frequency and user base size?	Please refer to GIC Re's response to Q.93
167	Advanced Audit (Optional): 1.CSPM - Which cloud platforms (AWS/Azure/GCP)? 2.AI/ML Audit - Any AI/ML systems in scope? 3.API Security - Number of APIs and integrations? 4.ISO 27001 - Current maturity level? Is gap assessment or certification required?	1.Please refer to GIC Re's response to Q.94; 2.Please refer to GIC Re's response to Q.33; 3.Please refer to GIC Re's response to Q.34; 4.Please refer to GIC Re's response to Q.35.
168	Will re-testing cover all findings or only critical ones?	Please refer to GIC Re's responses to Q.22 & Q.37.
169	Tools & Licensing: 1.Should bidder use own tools or client tools? 2.Any restrictions on open-source/commercial tools?	Please refer to GIC Re's response to Q.152.
170	How will additional scope (new apps/APIs) be handled?	Please refert to GIC Re's response to Q.34, Q.85 & Q.149.