युनाइटेड इंडिया इंश्यूरेन्स कंपनी लिमिटेड

UNITED INDIA INSURANCE COMPANY LTD.

At United India, It's always U before I

Pre-bid replies for REQUEST FOR PROPOSAL (RFP) FOR "Appointment of Auditor for Comprehensive Information & Cyber Security Audit, Red Team Exercise and Forensic Services"

TENDER NO: 000100/HO IT/RFP/2/2024-2025, GEM BID NO: GEM/2024/B/5019530

RFP Page No	RFP Clause No.	Description in the tender	Query/Suggestions	UIIC Responses
		General Queries	Are there any third parties involved? What kind of services are taken from third parties?	Details will be shared with the successful bidder
		General Queries	Is your infrastructure on cloud/ on prem? If on cloud, which deployment model is used and the cloud service provider?	Our infrastructure is on-prem as of now.
		General Queries	As per our understanding, implementation of any technology solution, applying patches is out of scope. Kindly confirm.	Applying patches is considered as IT support service
		General Queries	In the case of application doesn't response during application assessment, How penalty will be calculated?	Penalty is not applicable in such cases. However, it is the responsibility of the selected bidder to prove the same.
		General Queries	What is the buffer time that will get to initiate the activity?	In case of yearly activities like VAPT, Red Team & process audits, calendar will be shared well in advance. But for ad hoc activities (except forensic services)15 days buffer period will be given to initiate the activity
		General Queries	How the PO will be issued - Considering this is yearly and multiple services. Can we consider for each service a separate PO will be issued ?	Multiple Purchase orders will be issued. Some activities can be included in a single PO. Exact details will be shared with the selected bidder
		General Queries	What is the total duration on the validity ?	The contract is for a period of 2 years. Hence, validity will also be for a period of 2 years from the date of agreement.

		General Queries	Bidder will not require to draft and finalize of policies pertaining to applicable scope areas. Please clarify.	No.
7	1.2	General Queries	We assume that awareness trainings will be delivered only in English language. Is multilingual requirement also in scope? If so, kindly list down the languages.	Trainings shall be given in English and Hindi languages.
10	2.1 (c)	VAPT of application and network devices (black box)	Please let us know on the approximate sizes of applications hosted externally and internally.	Details will be shared with the successful bidder
10	2.1 (c)	VAPT of application and network devices (black box)	Is black box testing only for external applications or for both internal & external as well. Did UIIC prefers Configuration Review as a part of the scope	Black box testing is for both internal & external applications. Configuration review is not part of the scope.
10	2.1 (c)	VAPT of application and network devices (black box)	Please provide us the segregation of external & internal applications across different categories including mobile applications.	Details will be shared with the successful bidder
10	2.1 (c)	VAPT of application and network devices (black box)	Will this include identification of known vulnerabilities at code level (Software composition Analysis)	Software composition analysis is not part of the scope
10	2.1 (a)	General Queries	Given that the review has to be performed at multiple places across multiple different processes and systems, we shall work with UIIC to decide the sample size mutually. Also, please confirm if the DC-DR site visit is required	Accessibility to all IT infrastructure will be given from Head Office. However DC, DR and NDR visit is required to review physical security.
12	2.1 (d)	General Queries	What is the number of current policies and procedures in place	Exact details will be shared with the selected bidder.
12	2.1 (d)	General Queries	What are the current processes for financial reporting and ensuring solvency as per IRDAI guidelines?	Details will be shared with the successful bidder

12	2.1 (d)	General Queries	Are there any other regulations that need to be mapped to ISMS requirements other than IRDAI	Selected bidder should also check for compliance with Cert-in guidelines
12	2.1 (d)	General Queries	Please provide the overview of UII's information security policies and how they comply with ISO 27001:2022?	Details will be shared with the successful bidder
12	2.1 (d)	General Queries	Can you provide detailed records of compliance with IRDAI regulations? How are these compliance checks conducted?	Details will be shared with the successful bidder. Bidder can refer to IRDAI CS Guidelines, 2023 and corresponding audit checklist for reference.
12	2.1 (d)	General Queries	Is there any training and awareness sessions for ISO 27001:2022 to be conducted by Bidder? If yes then specify the details related to the same	This can be considered as part of training and awareness. Details will be discussed with successful bidder
12	2.1 (d)	General Queries	Is there a Risk Assessment Methodology already in place and when was it last reviewed?	Details will be shared with the successful bidder
12	2.1 (d)	General Queries	Please specify the timeline by which you expect to get ISO 27001 Certification. If you need any support from bidder for the certification	Details will be shared with the successful bidder. Support for ISO certification is not part of the scope
13	2.2 (a,b)	General Queries	What are security controls devices present (Antivirus, EDR/XDR, Firewall, IDS/IPS, DLP etc.)	Details will be shared with the successful bidder
13	2.2	General Queries	Is there any SOC (Security Operation Center) team or SIEM solution in place. If Yes, is it integrated with all the assets.	Details will be shared with the successful bidder
13	2.2	General Queries	What is the average EPS (events per second) getting observed.	Details will be shared with the successful bidder
13	2.2	General Queries	What is the average retention period of event logs.	Details will be shared with the successful bidder

13	2.2	General Queries	Is there any security solution available to capture and store flow logs.	Details will be shared with the successful bidder
13	2.2	General Queries	What are the underlying operating systems (eg: Windows, Ubuntu etc.) and Virtualization application (eg: ESXI, vcenter etc.) present in the environment.	Details will be shared with the successful bidder
17	2.2 (f)	General Queries	Any existing Incident Response plan in place?	Yes
17	2.2 (i)	Social Media Forensics	Performing Social Media Intelligence to verify the authenticity of the information.	As per RFP
18	2.2 (L)	Note	Need clarification on the Out of pocket expenses , How UIIC will be doing the reimbursement on the Out of pocket expenses or it will be on Actuals?	As per RFP. UIIC shall not reimburse any out of pocket expenses.
19	2.3	Red Team Exercise	Is SOC evaluation a part of red teaming assessment	No. SOC evaluation is not part of red team exercise.
19	2.3	Red Team Exercise	Did UIIC prefer both black box and grey box for red teaming exercise	Black box external red team exercise to be performed.
19	2.3	Red Team Exercise	Preferred location for Physical security for red teaming exercise.	Head Office, Chennai
19	2.2 (L)	Note	Should data processing occur at the client's location or within our own laboratory? (As computing power and tools are limited for processing data at client)	Data can be processed at selected bidder's lab.
19	2.2 (L)	Note	Regarding data retention, should we retain it internally or share it with the client after completing the activity?	Data should be shared with UIIC after completing the activity. Bidder should not retain UIIC's data.
19	2.2 (L)	Note	Basis the Regulatory and Risk requirement should the bidder will be performing the Analysis of the Information collected from all sources within the	Selected bidder can perform the analysis within the bidders lab environment.

			premises of the UIIC and Bidder can perform the analysis of the information within the Bidders lab environment.	
19	2.2 (L)	Note	In reference to the commercial terms of the RFP basis the rate card Bidder will have to provide the man hours rate card for the digital forensic activity .	As per RFP.
19	2.2 (L)	Note	Basis the Regulatory and Risk requirement should the bidder will be performing the Analysis of the Information collected from all sources within the premises of the UIIC and bidder can perform the analysis of the information within the Bidders lab environment.	Selected bidder can perform the analysis within the bidders lab environment.
20	2.4	Training Delivery	We understand that UIIC is looking for Cyber Awareness trainings in the following modes: A. Onsite Classroom training B. Virtual training Are you also looking for: C. Online trainings hosted and tracked via Learning Management System	UIIC is looking for Cyber Awareness trainings in the following modes only: A. Onsite Classroom training B. Virtual training
20	2.4	Training Delivery	In case of B. Virtual training requirement, it is assumed that the tools/software (Example: Ms-Teams, Zoom etc.) will be provisioned by UIIC. Is our assumption correct?	Yes online tools will be provided by UIIC
20	2.4	Training Delivery	In case of C. Online training requirement, does UIIC has an online Learning portal or the same has to be implemented/provisioned by the bidder?	Not part of the scope

20	2.4	Training Delivery	In case of C. Online training requirement, if the Learning Management System(LMS) has to be implemented; is UIIC ok with open source on premise implementation? And in such case, will UIIC provide the hardware/software infrastructure? Or is UIIC looking for a cloud based LMS implementation?	Not part of the scope
21	2.4	Feedback Mechanism	How does UIIC plan to capture the feedbacks from the learners? Ideally, this is managed using a standard LMS platform by capturing the feedbacks for every online course.	Details will be shared with the successful bidder
21	2.4	Questionnaire Provision	How does UIIC plan to use the Questionnaire template in order to evaluate the performance of learners? Ideally, this is managed by conducting quizzes at regular intervals using a standard LMS platform.	Details will be shared with the successful bidder
33	4.8	Sub Contract	We understand that subcontracting is strictly restricted under this engagement. In case of cloud based LMS provision (if opted for), there might be a need for bidder to collaborate with a licensed partner for providing such services. Is this arrangement permissible?	LMS is not part of the scope
33	4.8	Sub Contract	If opted for online training modules, every module must have a narration voiceover which needs to be recorded in a studio using artists. bidder already has on boarded subcontractors for availing	LMS is not part of the scope

			such services. Is this arrangement permissible?	
53	5.6 (9th point)	Annexure 6: Bill of Material	Bidder to factor the all its expenses we will need clarification apart from Amount specified	As per RFP. UIIC shall not reimburse any out of pocket expenses.
55	5.6	Summary of Costs [Commercial Bid]	It is mentioned that 8 units of Virtual trainings with each unit of 2 hours must be delivered under this engagement. If 16 hours of training has to be delivered under this engagement, what would be the ideal split among the delivery modes? Example: A. Onsite Classroom training- 6 Hrs B. Virtual training- 6 Hrs C. Online trainings- 4 Hrs	Details will be shared with the successful bidder
10	2.1 2.1. VAPT & IRDAI COMPLIANCE AUDIT	All the testing is to be conducted from UIIC HO located at Chennai. For IT systems located at locations other than at Chennai, HO, testing to be performed using remote connection. UIIC will facilitate the selected vendor for setting up the remote connection.	Could you please confirm whether the bidder is required to deploy a team onsite, or if there is provision for conducting VAPT (Vulnerability Assessment and Penetration Testing) remotely on internet-facing applications and servers	VAPT can be conducted remotely on internet facing applications & servers
13	2.2. DIGITAL FORENSICS	United India Insurance Company Ltd proposes to appoint firm for providing digital forensic services. The scope of engagement includes:	We understand that the bidder is expected to provide forensic services as per the specified scope when required. Could you please confirm whether a separate purchase order will be issued for these services? Your confirmation on this matter would be appreciated	Yes purchase order will be issued separately

20	2.4. TRAINING & EMPLOYEE AWARENESS (Optional)	Training Delivery:	Could you please confirm the frequency of training sessions required per year from the bidder? We assume that the training conveyance expenses will be borne by UIICL, and arrangements for onsite trainings will be made as necessary.	Training conveyance will not be paid separately. Arrangements for onsite training will be made by UIIC.
50	5.5 Annexure-5: Eligibility cum Technical Criteria	The bidder should be empaneled with CERT- IN for the period 2024-2025 for providing VAPT, IS Audit, Red Team and Forensic Services	we request you to reiterate the eligibility and technical criteria, specifically confirming that the bidder must have a valid CERT-IN empanelment as of the current date	Please refer corrigendum - 1
NA	NA	Extension request	We kindly request an extension of the bid submission deadline by at least 2 weeks. This additional time will allow us to prepare and submit a compliant and comprehensive proposal.	Please refer corrigendum - 1
49	The average annual bidder turnover from India operations in cyber security services should not be less than 4 Crores in each of the preceding 3 years - 2021-2022, 2022-2023, 2023-2024	Audited Annual Report/ Certificate from Chartered Accountant for the financial years 2021-2022, 2022-2023, 2023-2024 which includes profit and loss account and balance sheet.	Our Annual Report F Yr. 2023-24 has not been finalized yet. So, Can we provide the data for las three F Yr. 2020-2021,2021-2022,2022-2023	Please refer corrigendum - 1
50	The bidder should have a positive net worth in all the 3 preceding financial years - 2021-2022, 2022- 2023, 2023-2024	Audited Annual Report/ Certificate from Chartered Accountant for the financial years 2021-2022, 2022-2023, 2023-2024 which includes profit and loss account and balance sheet.	Our Annual Report F Yr. 2023-24 has not been finalized yet. So, Can we provide the data for las three F Yr. 2020-2021,2021-2022,2022-2023	Please refer corrigendum - 1
50	The bidder should have made profit in at least 2 years in the last 3 financial years - 2021-2022, 2022-2023, 2023-2024	Audited Annual Report/ Certificate from Chartered Accountant for the financial years 2021-2022, 2022-2023, 2023-2024 , which includes profit and loss account and balance sheet.	Our Annual Report F Yr. 2023-24 has not been finalized yet. So, Can we provide the data for las three F Yr. 2020-2021,2021-2022,2022-2023	Please refer corrigendum - 1

50	The bidder should be empaneled with CERT-IN for the period 2024-2025 for providing VAPT, IS Audit, Red Team and Forensic Services	Certificate of Empanelment with CERT- IN	We are in process of empanelment for the year 2024-25	Please refer corrigendum - 1
51	Details of proposed team, their experience, SPOC for each activity.		Please specify how many No. of resources required	Bidder should understand the scope of the work and deploy sufficient resources.
	EPT		Need no. of Public IP Addresses	Approximately 80±10. However, exact count will be shared with successful bidder
	Extension		Please extend due date of submission of tender for at least one week, after corrigendum we need time for preparation.	Please refer corrigendum - 1
10	2.1 (b) Tentative Infrastructure for Audit	Applications (Application VAPT)	In the scope we understand that 40 to 50 Applications for App PT activity. Please confirm the sizes of each application along with type of application (Web/Android/iOS) ***Small Size App(Less than 40 menus)** ****Medium Size App(Between 40 - 80 menus)** *****Large Size App(Above 80 menus)**	Since this is a black box testing, the number of web pages for each application may not exceed three. Only UIIC corporate website has more menus. Bidder can visit UIIC corporate website for understanding the size. Currently, we have one mobile app.
10	2.1 (b) Tentative Infrastructure for Audit	API	Kindly confirm if the 30 to 40 APIs provided for API Testing Activity are API Calls or API Domains. If they are API Domains, please confirm the total count of API Calls in these 30-40 API Domains	These are API calls.
10	2.1 (b) Tentative Infrastructure for Audit	Servers	Kindly confirm whether 200 to 220 servers provided for Network VAPT activity are Internal or External.	They include both internal and external

10	2.1 (b) Tentative Infrastructure for Audit	Authentication and Proxy Servers	Kindly confirm whether the servers (4 Authentication + 1 Proxy) provided for Network VAPT activity are Internal or External.	Details will be shared with the successful bidder
10	2.1 (b) Tentative Infrastructure for Audit	Desktops and Laptops	Kindly confirm if we have to consider 1000 Desktops and 150 Laptops for testing or if we can consider sampling. **If Sampling, please confirm the sampling Percentage to be considered.**	This will be discussed with successful bidder.
10	2.1 (c) VAPT of Applications and network Devices (Black Box)	External Applications	Kindly confirm the count of External Applications that have to be tested on a Half Yearly basis after the Annual VAPT	25±5
12	2.1 (d) Comprehensive Information and Cyber Assurance Audit (Annual Activity)	Scope of Audit	Please Highlight the count of locations in scope(**Ex: Corporate Office, Data Centers, DR Sites etc).**	Head Office, DC, DR and NDR
			Please highlight the count of Applications in scope and also brief about the applications	As per RFP
			Please highlight the count of Network Devices in scope	As per RFP
			Please highlight the count of Servers in scope	As per RFP
			Please highlight the number of departments in scope	As per RFP
			Please highlight the number of people in scope	As per RFP
			Please Highlight the Hosting of IT infrastructure **i.e., *In house Data Center/*Third Party Data Center Hosted(Physical Hosting Only/*Cloud Hosted)/*Third Party Data Center hosted & Managed.**	Our infrastructure is on-prem as of now. Further details will be shared with successful bidder
			Please mention the start date of the Project?	Will be shared with the successful bidder
			Please mention the expected end date of the project(Deadline)?	As per RFP

19	2.3 Red Team Exercise	Red Team Exercise	Please highlight the List of locations to be covered in scope.	Head Office and 3 offices. Locations of other three offices will be mutually discussed with selected bidder.
			Please highlight the No. of physical locations to be covered in scope	Head Office and 3 offices. Locations of other three offices will be mutually discussed with selected bidder.
			Please highlight the entities to be covered: *If there are multiple entities, please specify which entities need to be covered. (For example: "Cover only SISA India, not SISA Globe.")	Should cover United India Insurance Company Ltd India
			Please confirm, if you want to include an internal Red Team assessment? ***Internal Red Team: Assessing threats from inside to outside. *External Red Team: Assessing threats from outside to inside**	Only External Red Team exercise should be performed.
			Please highlight the type of approach: ***Time-boxed Approach: Continuous Red Teaming for a certain period (e.g., 6 months).** ***One-Time Assessment: Complete Red Team assessment within a defined timeframe.**	One time assessment within defined timeframe to be performed
20	2.3 Red Team Exercise	Deliverables	Kindly confirm what kind of compliance roadmap UIIC is looking for? Please provide a brief	As per RFP
20	2.4 Training and Employee Awareness	Training	Please highlight if any specialized trainings are required.	Will be shared with the successful bidder

10	2. SCOPE OF WORK (SOW)	LOCATION COVERED UNDER THE SCOPE , b) TENTATIVE INFRASTRUCTURE FOR AUDIT , c) VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VA/PT) OF APPLICATIONS AND NETWORKS DEVICES (BLACK BOX), d) COMPREHENSIVE INFORMATION AND CYBER SECURITY ASSURANCE AUDIT (ANNUAL ACTIVITY – TO BE CONDUCTED AT THE START OF EACH YEAR OR AS PER CONVENIENCE OF UIIC)	11. Are all devices accessible from 1 centralized location. 2. Require bifurcation of annual VAPT application and black box penetration testing for external applications. 3. Infrastructure of VAPT and Red team are same? Kindly confirm? 4. Are mobile applications also part of scope? Count required along with their platforms. Kindly provide the total number of vendors to be covered under the due diligence and Risk Assessment Audit. 5. What would be the location of the Audit 6. Whether the revalidation audit would be part of audit scope. 7. As part of Risk Assessment Audit, whether the VAPT need to be conducted at the vendor premises. If Yes, Details of the IT Infrastructure is required.	1. All devices are accessible from one location, however, selected bidder has to visit DC, DR and NDR 2. For annual VAPT infrastructure is already shared as part of scope. The count of external applications is 25+/-5 3. External Red team exercise should be performed. Hence, the infra will be limited to external facing applications and servers. 4. Yes. Currently we have one mobile applications available in google play store 5. Audit to be performed from UIIC Head Office. However, selected bidder has to visit DC, DR and NDR 6. Yes 7. Selected bidder need not audit at UIIC's vendor's premises. Vendor risk assessment is not part of the scope.
50	5.5 Annexure-5: Eligibility cum Technical Criteria Point 9	The bidder should have at least two Audit Consultants for each category below 1. CISA/CISSP qualified and should be continuously part of the team that will conduct the audit at UIIC 2. CEH qualified	Please elaborate	1. CISA/ CISSP qualified auditor should oversee and be part of the Compliance Audit. 2. CEH qualified shall be part of VAPT and Red team exercise.
50	5.5 Annexure-5: Eligibility cum Technical Criteria Point 10	The bidder should have at least five cyber forensic experts with relevant experience for a period of at least 5 years	Please confirm - Do we need to have experts or Experience for the audit conducted - If it is expertise then we request you Minimize it to 2 consultants instead of 5	Please refer corrigendum - 1

51	5.5 Annexure-5: Eligibility cum Technical Criteria Point 13	The bidder should have performed Red Team Exercise in at least 3 Govt./ PSU/ BFSI organizations in last three years	1. Please confirm can the current audit be considered 2. We request to add the regulators along with Govt./ PSU/ BFSI organizations in last three years 3. We understand that if we are conducting Red team audit for 2 separate years for same organization under a single agreement / PO, the same will counted as 2 instances. Kindly confirm 4. We request to minimize it to 2 instead of 3 audit	1. Current audit shall not be considered. 2. Please refer corrigendum - 1 3. Two separate exercise in the same PO will be considered as 2 instances. 4. As per RFP
51	5.5 Annexure-5: Eligibility cum Technical Criteria Point 14	The bidder should have provided cyber forensic services in at least 2 Govt./ PSU/ BFSI organizations in last three years	1. Please confirm can the current audit be considered 2. We request to add the regulators/ Banks along with Govt./ PSU/ BFSI organizations in last three years 3. We understand that if we are conducting Red team audit for 2 separate years for same organization under a single agreement / PO, the same will counted as 2 instances. Kindly confirm	1. Current audit shall not be considered. 2. Please refer corrigendum - 1 3. Two separate exercise in the same PO will be considered as 2 instances.
51	5.5 Annexure-5: Eligibility cum Technical Criteria Point 14	The bidder should have provided cyber awareness training services in at least 2 Govt./ PSU / BSFI organizations in last three years	1. Please confirm can the current audit be considered 2. We request to add the regulators/ Banks along with Govt./ PSU/ BFSI organizations in last three years	1. Current audit shall not be considered. 2. Please refer corrigendum - 1
62	5.11 Annexure 11:	Non-Disclosure Agreement	Do we need to submit it along with the bid or once the bidder is awarded	Selected bidder should submit NDA after bid is awarded.

68	5.12 Annexure 12:	Pre-Contract Integrity Pact (Format) (Bidders to submit 2 (two) copies of integrity pact in ₹ 100 stamp paper)	Do we need to submit it along with the bid or once the bidder is awarded	Should be submitted along with the bid.
50	5.5 Annexure-5: Eligibility cum Technical Criteria	The bidder should have at least five cyber forensic experts with relevant experience for a period of at least 5 years	Request you to kindly modify the criteria as: The bidder should have at least five cyber forensic/Red Teaming/VAPT experts with relevant experience for a period of at least 5 years	Please refer corrigendum - 1
10	2.1. VAPT & IRDAI COMPLIANCE AUDIT	5. UIIC Regional Offices, Learning Centre, LCBs, HUBs and Operating Offices at PAN India	Request you to kindly provide the count of each of the mentioned locations which is needed for effort estimation.	All devices are accessible from one location, however, selected bidder has to visit DC, DR and NDR for reviewing physical security
10	c) VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VA/PT) OF APPLICATIONS AND NETWORKS DEVICES (BLACK BOX)	Apart from annual VAPT, black box penetration testing for external applications should be conducted exclusively after six months from the date of completion of annual VAPT or as per convenience of UIIC. Revalidation should be conducted once the vulnerabilities are fixed or as communicated by UIIC	Kindly share the count of external applications to be considered for black box penetration testing	25+/-5
11	c) VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VA/PT) OF APPLICATIONS AND NETWORKS DEVICES (BLACK BOX)	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.	Kindly confirm if UIIC will be sharing the list of target applications and network devices along with their IP address.	Details will be shared with successful bidder
11	c) VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VA/PT) OF APPLICATIONS AND NETWORKS DEVICES (BLACK BOX)	Use tools to perform a password scan to determine accounts that have passwords that are "easy" to crack.	Kindly confirm if password spray attack for the entire active directory users is expected.	Can be done on sample basis. Details will be discussed with successful bidder

12	c) VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VA/PT) OF APPLICATIONS AND NETWORKS DEVICES (BLACK BOX)	Additionally, a compliance report should also be submitted once the gaps are closed.	Bidder will not provide any certificate of compliance. Bidder will provide the revalidation report in bidder's reporting format. Kindly confirm if the understanding is correct.	Agreed
13	d) COMPREHENSIVE INFORMATION AND CYBER SECURITY ASSURANCE AUDIT (ANNUAL ACTIVITY – TO BE CONDUCTED AT THE START OF EACH YEAR OR AS PER CONVENIENCE OF UIIC)	The Selected Bidder/ Auditor will provide Compliance Assessment Report / External Audit Completion Report covering Data Centres (Primary Site, NDR and DR Site), UIIC Head Office and other offices with respect to o UIIC Information Security Policy o IRDAI Guidelines on Information & Cyber Security o ISO 27001:2022 Guidelines o Software License Compliance (DC, NDR & DR) o Any other legal requirement	Bidder will not provide any certificate of compliance. Bidder will provide the revalidation report in Bidder's reporting format. Kindly confirm if the understanding is correct.	As per RFP.
13	d) COMPREHENSIVE INFORMATION AND CYBER SECURITY ASSURANCE AUDIT (ANNUAL ACTIVITY – TO BE CONDUCTED AT THE START OF EACH YEAR OR AS PER CONVENIENCE OF UIIC)	The Selected Bidder/ Auditor will provide Compliance Assessment Report / External Audit Completion Report covering Data Centres (Primary Site, NDR and DR Site), UIIC Head Office and other offices with respect to o UIIC Information Security Policy o IRDAI Guidelines on Information & Cyber Security o ISO 27001:2022 Guidelines o Software License Compliance (DC, NDR & DR) o Any other legal requirement	Kindly clarify on the expectations regarding Software License Compliance (DC, NDR & DR).	As per RFP

13	d) COMPREHENSIVE INFORMATION AND CYBER SECURITY ASSURANCE AUDIT	Compliance Assessment Report / External Audit Completion Report for IRDAI CS Guidelines released in April, 2023 and its subsequent amendments. Reports to be furnished as per the formats mandated by IRDAI	Bidder will not provide the report as per the formats defined by IRDAI instead Bidder will provide the report in Bidder's standard reporting format. Request you to kindly consider the same.	As per RFP
19	2.3. RED TEAM EXERCISE	Evaluating the effectiveness of physical and digital security controls.	1. Kindly confirm if physical security assessment is expected. 2. If yes, kindly confirm the number and locations in scope for physical security assessment	1. Yes 2. HO and any other three offices. The locations of these offices can be mutually discussed and agreed upon.
19	2.3. RED TEAM EXERCISE	Simulating various cyber threats, including social engineering attacks, phishing attacks and malware infiltration	As part of red team, phishing simulation will be limited to employee IDs gathered during the reconnaissance phase only. Kindly confirm on the understanding.	Yes
19	2.3. RED TEAM EXERCISE	Penetrating internal systems to assess their security posture.	1. Kindly confirm if a separate/parallel internal red team activity is expected along with the external red team activity. 2. if yes, kindly confirm if UIIC will be providing standard employee asset device to initiate the activity	1. External Red Team exercise to be conducted.
19	2.3. RED TEAM EXERCISE	Executing covert tests, such as phishing and wireless intrusion attempts.	1. Kindly confirm of Wi-Fi Security testing is expected. 2. If yes, kindly confirm the number of locations and SSIDs in scope.	1. Wi-Fi testing to be performed at HO 2. SSID details will be shared with successful bidder
20	2.3. RED TEAM EXERCISE	Deploying malicious emails with attachments to assess staff susceptibility.	1. Kindly elaborate on the expectation. 2. How many users to be targeted as part of this activity.	Number of users can be mutually agreed upon
24	3.3.2 Clarification of Tender document	The Representatives of Bidders attending the pre-bid meeting must have proper authority letter to attend the same and must have paid the Tender Fee	The tender fee is mentioned as Nil in the Schedule of events, kindly clarify on the expectations.	No tender fee is required

28	3.7 Evaluation of Bids	4. The evaluation shall be based on Eligibility Cum Technical Bid and Commercial Bid. UIIC at its discretion may ask bidders to give a presentation	Request you to kindly consider Quality and Cost based Selection (QCBS) for the evaluation of the bids with weightage as 80% for technical bid and 20% for the commercial bid.	As per RFP
49	5.5 Annexure-5: Eligibility cum Technical Criteria	3. The bidder must comply with procurement policy guidelines mentioned in https://cvc.gov.in/guidelines/tender-guidelines	There are multiple guidelines of CVC under Public Procurements. Request you to kindly provide the specific guideline name or the document.	As per RFP
49	5.5 Annexure-5: Eligibility cum Technical Criteria	4. The bidder should not be providing IT/IS implementation, support related service(s) to UIIC currently and should not have conducted IS Audit/ VAPT during the last 2 years (From Date of Issue of this RFP) for UIIC	We are currently assisting UIIC in undertaking digital initiatives for the next three years. We understand there will be no conflict with the current scope of work. Kindly let us know in case otherwise.	If the bidder is assisting in digital initiatives there is clear conflict of interest.
50	5.5 Annexure-5: Eligibility cum Technical Criteria	The bidder should have at least two Audit Consultants for each category below : 1. CISA/CISSP qualified and should be continuously part of the team that will conduct the audit at UIIC 2. CEH qualified	Bidder has sufficient numbers of resources who are qualified as CISA and CISSP. However, the deployment will be considered upon successful selection. Hence requesting you to modify the clause as below: The bidder should have at least two Audit Consultants for each category below : 1. CISA/CISSP qualified 2. CEH qualified	As per RFP.

Date: 24/06/2024

Place: Head Office, Chennai

UNITED INDIA INSURANCE CO. LTD.
IT DEPT.
HEAD OFFICE
CHENNAI