Response to Pre-Bid queries						
Tender Name: Request for proposal (RFP) for Appointment of Auditor for 2 Years for Conducting Information Security and Cyber Security Audit						
Ref No.	**IT-11/2023-24**					**Date: 05-Mar-2024**
S. No.	**Page No. & Reference Clause**	**Point /Section #**	**Category (Eligibility / Scope / Commercial / Legal / General)**	**Clause Details**	**Query/seeking clarification**	**Response**
1	9	Point 1	Eligibility Criteria	1. Eligibility Criteria The Bidder should have completed satisfactorily below audits/assessment for at least 03 (three) different companies each in India during last 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment	We need to submit at least 3 copies of LOI/PO/Work Order/Completion Certificate' from the client. Will it suffice if we provide 3 purchase orders? Also, are we allowed to provide client references from any region worldwide?	Yes, bidder can provide 3 PO copies for atleast 3 different companies for each audit conducted in India only.
2	13		General	E-sign ESP audit for UIDAI	We will follow the guidelines outlined in Section 2.3. If any additional information is required, please inform me.	No Change
3	13		General	CSGL System Audit for RBI	If we lack a subject matter expert, can we outsource the task or exclude it and provide a quote for the remaining services?	No outsourcing allowed. For every audit exercise, it is a IT system audit where activities to be audited are generic in nature and not specific to a domain. This is not a business process audit.
4	14		General	Custody System Audit The Insurance clients require an audit certificate from our Internal Auditors in which one of the confirmation is relating to System audit of Custody. Hence Annual System Audit is required from Auditor	Could you please provide further details on what is required? Additionally, is it possible to obtain a copy of last year report	Custody Audit Checklist is herewith shared
5	15		General	OWASP Top 10 API (Audit # 6): OWASP Top Ten criteria as mentioned below but not limited to –	Could you please provide the total number of applications that require testing?	This is specific to the API platform irrespective of the applications consuming/responding to the API. There is only one API Platform in StockHolding providing API services across 4 applications

6	16		General	Vulnerability Assessment and Penetration Testing	Could you please provide the number of internal and external IPs that require testing? Additionally, could you confirm whether we need to conduct an assessment of the operating system and database configurations?	External PT: 30 IPs, Internal PT IPs: 200
7	12		Scope of Work	Scope of Work	Could you please confirm the number of locations that need to be audited? Considering there are 210 branches, could we potentially conduct the audit on a sample basis?	Branches audit are not in scope. All applications are hosted at Data Centre hosted at Mahape, Navi Mumbai. Only for Red Teaming 2 Mumbai based branches are in scope. Please refer Page 21, Point 7
8	12		Scope of Work	Scope of Work	The audit can be conducted using a combination of both hybrid and onsite modes.	Only onsite mode is allowed except for external VAPT for internet facing applications , OWASP Top 10 Audit and External Red Teaming which can be done remotely (offsite)
9	12		Scope of Work	Scope of Work	Could you please confirm the number of People included in the scope?	Auditor has to confirm on the same
10	23		Commercial Bid	Commercial (Indicative Price) Bid	If our quotation increases in alignment with the estimated bid value, it would be considered reasonable and expected.	Price to be quoted is for period of 2 years of the contract value
11	23		General	L1 price will be based on Table A as mentioned in Annexure – 3	Do we have Reverse auctions ?	No
12	24		General	OWASP API Audit - API Audit	Please inform me of any APIs you developed in the month/year specified	This will be shared only with the winning bidder
13	9	Point 4	Eligibility Criteria	4. Audit Firm should be based within MMRDA region	Request you to kindly allow Audit firm within Pan India location	Audit Firm should be based within Maharashtra state

14	9	Point 6	Eligibility Criteria	6. The bidder should be empanelled with CERT IN for last 5 years from RFP date	Request to kindly modify clause as below: The bidder must be CERT-In empanelled security auditor organisation as on 31 October 2023/ should have already applied for the CERT-In empanelment Justification: "Also, to keep you posted that the CERT-In empanelment has expired on October 31, 2023, for which all the CERT-In empanelled firms/ companies had to submit their application for re-empanelment We have applied for empanelment with CERT-In under the umbrella of Mazars Advisory LLP as an IT Security Auditing Agency owing to restructuring in the firm (previously registered as “Mazars Advisory Private Limited”), which is expected to be completed by March. Further, we have cleared stage 2 and stage 3 is in process and is expected to be completed by March'24" OR Auditor must be holding certifications like CISA/DISA/Cert-in empanelled Auditors. OR The Bidder should be a Chartered Accountant firm shall be a Partnership Firm / Limited Liability Partnership (LLP) firm under the Limited Liability Partnership Act, 2008, registered with the Institute of Chartered Accountants of India (ICAI), who fulfil the following criteria: a. continuous practice of at least five years; b. a minimum of four partners before the date of appointment; c. at least one Partner shall be Certified Information Systems Auditor (CISA) / DISA of ICAI; d. at least one partner shall be a Fellow Member of the ICAI; e. at least one Partner shall have a minimum of three years of experience in Cyber Security/ Information Security review / Information Security audit of Government (Central/ State/ PSU)/ Private Sector/ Financial Institutions/ Banks/ Insurance Companies; f. at least one partner has the experience of audit in IT environment and in conducting Audit from remote location. OR The bidder must be empanelled with India Banks Association for Forensic Services	No Change
15			Additional Clauses for inclusion	Indemnity	Tenderer shall indemnify and hold harmless the bidder for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such Bidder.	No Change

16			Additional Clauses for inclusion	Limitation of the Bidder's Liability towards the Purchaser	Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive, or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. Tenderer (and any others for whom Services are provided) shall not recover from the Supplier, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	No Change
17			Additional Clauses for inclusion	Non-solicitation	Bidder shall not hire employees of Tenderer or solicit or accept solicitation (either directly, indirectly, or through a third party) from employees of Tenderer directly involved in this contract during the period of the contract and one year thereafter.	No Change
18			Additional Clauses for inclusion	Force Majeure	1) Bidder shall not be liable for forfeiture of its performance security, Liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. 2) For purposes of this Clause, "Force Majeure" means an event explicitly beyond the reasonable control of the Contractor and not involving the contractor's fault or negligence and not foreseeable. Such events may be due to or as a result of or caused by act of God, wars, insurrections, riots, earth quake and fire, revolutions, civil commotion, floods, epidemics, quarantine restrictions, trade embargos, declared general strikes in relevant industries, satellite failure, act of Govt. of India, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation. In the event of any such intervening Force Majeure, either party shall notify the other in writing of such circumstances or the cause thereof immediately within five calendar days. 3) Unless otherwise directed by Tenderer in writing, the selected contractor shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. 4) In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, Tenderer and the bidder shall hold consultations in an endeavour to find a solution to the problem. 5) Notwithstanding above, the decision of Tenderer shall be final and binding on the bidder regarding termination of contract or otherwise	No Change

19			Additional Clauses for inclusion	Termination for Convenience	1) In case of termination, Tenderer shall pay the bidder for all work-in progress, Services already performed, and expenses incurred by the bidder up to and including the effective date of the termination of this Agreement. 2) Tenderer shall be entitled to terminate/cancel the purchase order at any time for the balance order quantity which is within the delivery schedule with no liability on either side and without assigning any reason thereof. However, the purchase order for the quantity which has already been offered for inspection shall not be cancelled and supply of the same shall be availed in due course of time. 3) Bidder may terminate/cancel the contract by giving a written notice of 30 days in case: a) Its invoices are not paid on time b) If Tenderer fails to comply with the terms of agreement	No Change
20			Additional Clauses for inclusion	Retention of copies	On payment of all bidder fees in connection with the Contract, Tenderer shall obtain a non-exclusive license to use within its internal business, subject to the other provisions of this Contract, any Deliverables or work product for the purpose for which the Deliverables or work product were supplied. bidder retains all rights in the Deliverables and work product, and in any software, materials, know-how and/or methodologies that bidder may use or develop in connection with the Contract.	No Change
21			Additional Clauses for inclusion	Non-Exclusivity	It is agreed that the services are being rendered on a non-exclusive basis and the bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	No Change
22			General	WebApp	No. of web applications to be tested? Including subdomains if any. Eg.www.123.com, xyz.123.com	Between 5-7 web applications to be tested
23			General		No. of user roles within each application?	Approximately 3-5 user roles / application
24			General		No. of dynamic pages/screen within each application?	This information is not relevant this RFP
25			General		Web Application is Internal/External network facing? No. of internal and external apps?	This information is not relevant this RFP
26			General		Web Application to be tested- Onsite/Offsite?	Offsite for Web Application is allowed
27			General		Web Application testing approach to follow - Black box/Grey Box? **Black Box** - Only application URLs will be provided for the testing. **Grey Box** - All URLs/credentials/test data will be provided for the testing	This information is not relevant this RFP
28			General	Mobile App	No. of mobile applications to be tested?	This information is not relevant this RFP
29			General		No. of mobile platforms to be tested? Eg. iOS/Android	This information is not relevant this RFP
30			General		Mobile application testing approach - Black box/Grey Box? **Black Box** - Only .apk/.ipa mobile application files will be provided for the testing **Grey Box** - Mobile application files, credentials and test data will be provided for the testing.	This information is not relevant this RFP
31			General		SSL pinning and Jailbreak/root detection is enabled on all mobile platforms (iOS/Android) ?	This information is not relevant this RFP

32			General		No. of user roles within each mobile application?	This information is not relevant this RFP
33			General		No. of dynamic pages/screen within each mobile application?	This information is not relevant this RFP
34			General	API	Number of external APIs in the scope?	This information is not relevant this RFP
35			General		Number of methods?	This information is not relevant this RFP
36			General		Approach for API testing, grey box or black box?	This information is not relevant this RFP
37			General	Infra VA	Number of external IPs	30
38			General		Number of Internal IPs	200
39			General		Is credential scanning expected?	Yes
40			General	Infra PT	Number of external IPs	30
41			General		Number of Internal IPs	200
42			General		Is credential scanning expected?	Yes
43			General	Firewall	Do you need to conduct firewall secure configuration review?	Yes
44			General		Total no. of Firewalls for review?	26
45			General		Please provide name and version details of each Firewall.	Firewall OEM and version details will be provided to Successful bidder.
46			General		Do you need to conduct firewall ACL rule set review?	No
47			General		If yes, total number of firewall ACL rules to review?	Not Applicable
48			General		Will you provide internal firewall security baseline documents to refer?	Bidder should use CIS Benchmark Level 2
49			General		Activity will be onsite/offsite?	OnSite
50			General		Could you share firewall configuration files with our offsite team?	No
51			General	Network Devices and Solutions	Do you need to conduct secure configuration review of networking devices?	All the Servers including AD /SCCM , DC /DR/NDR Fort and CP network Routers, Switches and all Network security devices.
52			General		If yes, No. of routers to review?	DC /DR/NDR Fort and CP network Routers = 10
53			General		No. of switches to review?	DC /DR/NDR Fort and CP network Switches = 30
54			General		No. of other network devices to review	Not Applicable
55			General		Do you need to conduct secure configuration review of network/security solutions?	YES
56			General		Total No. of security/network solutions to review?	120
57			General		Name and version of all network/security solutions to review? Eg. WAF BIG-IP 16.1.2	To be provided to successful bidder
58			General		Will you provide organisation internal security baseline documents for above solutions?	Bidder should use CIS Benchmark Level 2
59			General		Activity will be onsite/offsite?	Onsite
60			General		Could you share solutions configuration files with our offsite team?	No
61			General		Do you need to conduct secure configuration review on servers?	YES

62			General	Servers	If yes, Total No. of servers (App/web/DB/OS) to conduct secure configuration review?	200
63			General		Please provide name and version of all server platforms for review. Eg. Windows server 2016, MSSQL 2012, IIS10 etc.	Windows 2012,2016,2019,2022, Redhat Linux , Oracle Linux,Oracle 19C Database MSSQL 2016
64			General		Will you provide organisation internal security baseline documents (SCD/MSB) for review?	Bidder should use CIS Benchmark Level 2
65			General		Activity will be onsite/offsite?	Onsite
66			General	External Assessments	Could you please provide a tentative asset count for the following items?	
67			General		Number of Servers:	160
68			General		Number of Users:	5
69			General		Number of Locations:	2
70			General		Number of Departments:	15
71			General		Regarding social engineering, what is the expected number of scenarios to be covered?	StockHolding should have an approved Social Media Policy
72			General		For social engineering, how many users are to be considered?	Not Applicable
73			General	Internal Assessments	Can we obtain the necessary testing access, if it becomes necessary?	No access will be provided and is not required
74			General		How many distinct geographical locations are included?	Branches audit are not in scope. All applications are hosted at Data Centre hosted at Mahape, Navi Mumbai. Only for Red Teaming 2 Mumbai based branches are in scope. Please refer Page 21, Point 7
75			General		Are we expected to cover a physical breach or physical penetration test? If so, how many geographical physical locations should be taken into account?	No
76			General	Time Period	Is it obligatory to complete the respective activities within the timeline?	Yes
77			General		How many locations are covered in scope of various audits?	Branches audit are not in scope. All applications are hosted at Data Centre hosted at Mahape, Navi Mumbai. Only for Red Teaming 2 Mumbai based branches are in scope. Please refer Page 21, Point 7
78			General		How many in-scope business units, or departments at each location?	15
79			General		How many people at each location?	This information is not relevant this RFP
80			General		Number of Applications which are in scope of the Audits?	This is already mentioned
81			General		Number of IT devices, Network Devices, Security Devices?	200

82			General	GRC	Number of outsourced vendors in the scope department?	This information is not relevant this RFP
83			General		Please share the scope of Custody System Audit.	Custody Audit Checklist is herewith shared
84			General		What is the scope defined for the ISO 27001 certification?	Information Security Management Systems Related to Data Center and its Operation As per the Statement of Applicability of 20.12.2021 Version 2.3
85			General		Mention any existing IT/IS standard/Certification in place, if yes mention scope	ISO27001:2013 certified, SOC2 Certified
86			General		Are they already certified / audited previously for SSAE18 - SOC2 Type 2 or this is first time implementation?	Already certified
87			General		Is this an onsite audit?	Only onsite mode is allowed except for external VAPT for internet facing applications , OWASP Top 10 Audit and External Red Teaming which can be done remotely (offsite)
88			General		Is implementation support of identified findings also required?	No. This will be handled by StockHolding
89		Point 2	Eligibility Criteria	The bidder should have an annual turnover of at least Rs. 2 Crores per annum for last three financial years (2010-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies.	Is it possible to relax this criteria to Rs. 1 crore for any of 2 years in last 3 years. At 2 crores, we do not qualify.	No Change
90		Point 5	Eligibility Criteria	The Bidder should have completed satisfactorily below audits/assessment for at least 03 (three) different companies each in India during last 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment		

91		Point 6	Eligibility Criteria	The bidder should be empanelled with CERTIN for last 5 years from RFP date Certificate of Empanelment with CERTIN for last 5 years from RFP date	All the above means a firm must be CERT-In empanelled for last 5 years (we are empanelled with CERT-In since 2005 without break) and also must be registered with ICAI (which we are not as we are not an CA firm). Further, you are asking at least 5 auditors having ICAI/ AICPA (This is American) membership. This means that only CA firm with at least 1 CPA can apply. Firm, which are promoted and managed by Technologist may not be eligible. CERT-In or any other audit does not impose any such requirement of ICAI or AICPA membership. Thus, we request you to allow to quote for only any of the three services. We would like to quote for all IT audits ONLY. (Ideally, SOC 2 is required mostly in US and Canada. Unless you are catering to US or Canadian clients, SOC 2 may not be mandatorily required).	No change in Eligibility Criteria for point 5. No change in eligibility criteria for point 6. Point 7 in Eligibility Criteria - Removed Point 8 in Eligibility Criteria modified. Refer Annexure - 2: Eligibility Criteria in Corrigendum - 1. For SOC-2 Audit, Bidder to arrange Certified Audit report duly attested from certified member of ICAI/CPA. Attestation can be outsourced.
92		Point 7	Eligibility Criteria	For SOC 2 Audit: Bidder should be registered with the Institute of Chartered Accountants of India (ICAI) Valid Certificate for ICAI membership		
93		Point 8	Eligibility Criteria	The bidder should have on payroll – 1. For IT Audit : at least 5 Auditors who are CISA/CISSP qualified or equivalent; 2. For SOC-2 Audit : at least 5 Auditors having ICAI / AICPA membership; 3. For Red Team Assessment : at least 05 Offensive Security Certified Professional (OSCP) from offensive security / Certified Ethical Hacker (CEH) from EC-Council / Licensed Penetration Tester (LPT) from ECCouncil / GPEN: GIAC Penetration Tester from SANS / GWAPT: GIAC Web Application Penetration Tester from SANS / any other Red Team or Penetration Testing related certification; All Relevant certificates/documents supporting basis laid out in prequalification criteria.		
94			General		During pre-bid meeting – you said that the firm must quote for all three services and part quote is not acceptable.	Yes
95			General		Should organization bid for all activities or can go for specific activity like only for IT audit?	Bidder has to quote for all 3 activities
96			General		For SOC 2 audit, IT is compulsory that at least 5 Auditors having ICAI / AICPA membership?	Point 8 in Eligibility Criteria modified. Refer Annexure - 2: Eligibility Criteria in Corrigendum - 1.

97			General		Due to dependency of the activity as part of the contract, will there be any opportunity for the extension of the contract (beyond specified contract period)	No extension of contract beyond 3 years
98			General		Whether it is necessarily an onsite work requirement or a hybrid approach can be taken, need-based?	Only onsite mode is allowed except for external VAPT for internet facing applications , OWASP Top 10 Audit and External Red Teaming which can be done remotely (offsite)
99			General		Whether multiple sites/out-of-station sites have to be covered for the audits? If yes, what are the locations?	Branches audit are not in scope. All applications are hosted at Data Centre hosted at Mahape, Navi Mumbai. Only for Red Teaming 2 Mumbai based branches are in scope. Please refer Page 21, Point 7
100			General		How much time gap would be there between the draft report submitted and the restart of the revalidation audit?	Only in case of VAPT, GAP would be 90 days. For other Audits, it would be between 7 days to 90 days depending on the audit point to be rectified
101			General		Can you reduce the number of Offensive Security Certified Professionals (OSCP) to 3?	No Change
102			General		Can ICAI be outsourced?	SOC2 Activity has to be conducted by the bidder. Attestation can be outsourced.
103		Point 2	Eligibility Criteria	The bidder should have an annual turnover of at least Rs. 2 Crores per annum for last three financial years (2010-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies.	You have mentioned the clause regarding turnover of 2 crores for any organization, so we are not able to fulfil this clause, and organization has been registered in MSME. Please confirm to us that we may participate in tender whether or not.	MSME exemption for turnover and EMD only is applicable
104		Point 4	Eligibility Criteria	Audit Firm based within MMRDA region - Registered office Address Proof (Self-certified Copy) submitted	We have an branch office in Pune Balewadi. So please let us know if you can give us some relaxation on this. Our Head Office is in Ahmedabad Gujarat.	Audit Firm should be based within Maharashtra state

105		Point 5	Eligibility Criteria	Completed audits/assessment for at least 03 different companies each in India during last 05 years i.e. 2018-19, 2019-20, 2020-21, 2021-22 & 2022-23. 1. IT Audit 2. SOC 2 Audit 3. Red Team Assessment - Never	Yes, if these services can be relaxed to 1 year	No Change
106		Point 6	Eligibility Criteria	Empanelment with CERT-IN for the last 5 years from RFP date (3 year)	From Last 3 years	No Change
107		Point 7	Eligibility Criteria	Registered with the Institute of Chartered Accountants of India (ICAI) for SOC 2 Audit - We are not registered	Not Registered. So if you can give us relaxation	SOC2 Activity has to be conducted by the bidder. Attestation can be outsourced.
108		Point 7	Eligibility Criteria	Valid Certificate for ICAI membership submitted - Not Registered	Not Registered. So if you can give us relaxation	SOC2 Activity has to be conducted by the bidder. Attestation can be outsourced.
109		Point 8	Eligibility Criteria	On Payroll - For IT Audit: at least 5 Auditors who are CISA/CISSP qualified or equivalent - Yes	Not Registered. So if you can give us relaxation	No Change
110		Point 8	Eligibility Criteria	On Payroll - For SOC-2 Audit: at least 5 Auditors having ICAI/AICPA membership No	Not Registered. So if you can give us relaxation	SOC2 Activity has to be conducted by the bidder. Attestation can be outsourced.
Note: All other clauses/Terms & conditions except above shall remain same as per RFP (RFP Reference Number: IT-11/2023-24)						