Empanelment of Digital/Cyber Forensic Investigation/Audit Service Provider for a period of THREE years through RFP process for availing:

1) Digital/Cyber Forensic Readiness Assessment of our bank in order to analyse, identify and mitigate the deficiencies, if any, in the Forensic Incident handling, log collection and storage capabilities

2) On-demand Digital/Cyber Forensic Services in order to investigate a computer/cyber incident, analyse the root cause, identify the intruder and provide assistance to the Bank's Legal team with presentable evidences for prosecution of the perpetrator in a court of law in the event of any incident.

RFP No: IB:CO/ISSD/259/2021-2022 **DATED:29/10/2021**

REPLY TO QUERIES RAISED BY BIDDERS IN THE PRE BID MEETING HELD THROUGH WEBEX ON 09.11.2021 at 15:30 hrs

---

Sr. No.	Referred Point/Clause No.	Point	Queries raised by Bidders	Bank's Replies to queries
1	2.1	Scope of Digital/Cyber Forensic Services	How many applications/services will be considered for Forensic Readiness Assessment and Incident Audit Services?	Bank's IT infrastructure-Major items like CBS, Delivery Channels (ATMs, IB, MB, UPI etc.), Aadhar Enables Payment system, SWIFT, IMPS, RTGS, NEFT etc. among others. List of critical applications will be provided during the assessment time.
2	2.1	Scope of Digital/Cyber Forensic Services	Forensic analysis and Incident response services to be provided in which all locations? Is there any overseas work?	IT Infrastructure in India (Branches, Admin Offices & Data Centres) where the incident is reported.

3	2.1	Scope of Digital/Cyber Forensic Services	Does the Bank agree to perform analysis of the collected data and the password recovery of encrypted data in bidders Forensic labs? Expert testimony refers to expert witness services?	YES. With proper NDA and Agreement
4	2.1	Scope of Digital/Cyber Forensic Services	Will the shipment cost be borne by the Bank?	No
5	2.1	Scope of Digital/Cyber Forensic Services	After the collection of evidence and analysis, where does the bank expect the bidder to store the evidence?	Chain of custody shall be maintained as per the NDA and agreement
6	2.1	Selected Digital/Cyber Forensic Audit Services Provided is expected to	Does the Bank have any existing policies in place for Digital Forensics Collection, Incident Response and evidence storage?	Yes
7	2.1.A	Scope of Digital/Cyber Forensic Services Readiness Assessment	How many critical applications and infrastructure services does the Bank expect the bidder to perform Readiness Assessment on?	Bank's IT infrastructure-Major items like CBS, Delivery Channels (ATMs, IB, MB, and UPI etc.), Aadhar Enabled Payment system, SWIFT, IMPS, RTGS, and NEFT etc. Among others. List of critical applications will be provided during the assessment time.

8	2.1.A	Scope of Digital/Cyber Forensic Services Readiness Assessment	What is the period for which the bidder is expected to verify the historic logs on sample basis evaluated by the Bank's IT team?	As per the bank's retention policy and as per the requirement of the reported Incident investigation.
9	2.1.B	Scope for conduct Digital/Cyber Forensic Incident Audit/Investigation Analysis	Does the bank provide hand held devices to its employees?	Laptops & TABs are given to employees and Bank's service providers as per requirement which are connected to Bank's network through VPN /PIM as per the specified SOP.
10	2.1.B	Scope for conduct Digital/Cyber Forensic Incident Audit/Investigation Analysis	Has Bank authorized the use of any cloud storage services by the employees to share/store Bank data?	Sensitive information
11	2.3	Conduct of Audit	Which all locations are expected to be covered in the Audit?	Primarily Chennai & Mumbai. Branches & other offices as in case to case basis if required.
12	3	Digital/Cyber Forensic Assessment /Incident Audit Universe	How many POS devices, ATMs/Cash Deposit Machines, Network devices and end point devices are to be considered for the audit?	Based on requirement only
13	-	-	Can we change the resources for each incident or only named profiles are required?	Bidder may assign the task to the assigned proposed team members only. However, if for any reason some team member is to be replaced/substituted, the

				same may be done with prior permission/intimation to the Bank and the replacement member must have suitable equivalent qualification as per the RFP requirement.
14	-	Commercial Bid Format	10 man days for Forensic readiness services are too short, hence are we going to revise it? For On demand forensic services, if the hours exceeds more than 25 then the same man-day rate will be applied for additional hours?	Forensic Readiness Assessment is the core part of the Retainer-ship Activity amount (Part A) of the Commercial Bid, where man-days are not applicable. 10 man days included in Part A i.e. Overall Retainer ship amount, is to be utilised for On-Demand Forensic Investigation Services only as and when an incident occurs and the same is not chargeable.
15	-	Commercial Bid Format	In case of evidence collections, will the cost of the required storage media be borne by the Client?	All-inclusive by bidder
16		Commercial Bid Format	Out of Pocket expenses such as travel cost, other incidental expenses, external hard drives cost etc. shall be considered separately?	For Forensic Readiness Assessment the Cost will be all inclusive. No Extra TA/DA etc. would be entertained. For On Demand Forensic Investigation services at any place in India, only actual travelling expenses via Flight (Economy Class) /Train (Second AC)/ Bus etc. as

				applicable would be payable for reaching the incident site. Boarding/lodging charges would be borne by the Bidder.
17	8.3	The Bank intends to engage those applicants who are included in the latest panel of Information Systems Auditors maintained by Computer Emergency & Response Team, India [CERT-IN] as on date, preferably having Digital / Cyber Forensic Analysis and Investigation capability as one of the specialized /Core Competence areas of operation.	Do we need to submit the Cert-In empanelment Certificate or there will be an Annexure that we need to submit along with the bid? No Format available for DOC-G available in the tender document	Current valid CERT-In Empanelment Certificate only to be uploaded
18	8.4	The applicant should have positive net worth and should have turnover of more than Rs 10.00 Crores from IT Security/Audit Services in each of the last three Financial years (FY 2021-2020,FY 2020-2019 & FY 2019-2018)	We request you to kindly relax the criteria to 8 crores as MSME organizations have relaxations as per the Policy Circular No. 1(2)(1)2016-MA dated 10th March 2016.This point can be waived as per the new amendment in MSME vide Policy Circular No. 1(2)(1)2016-MA dated 10th March 2016. Circular copy along with MSME certificate attached for your perusal. (Circular attached)	The Annual turnover of the Bidder should be minimum Rs. 8 crores (Rupees Eight Crores) in each of the last three Financial years (FY 2021-2020,FY 2020-2019 & FY 2019-2018)
19	8.5	The Prospective team should have minimum 10 resources with minimum 5 years of experience in IT Security domain/Digital Cyber Forensics having any of the following certifications - CISA / CISSP /CEH/CISM with at least 2	We have understood the scope of work and request you to kindly reconsider the professional required with certifications. As per the scope of work the professional required seems to carry out the assessment could have:-Total certified	The proposed team should have 10 members with - CISA / CISSP /CEH/CISM out of which at least 2 individual resources must have any of the additional Professional Forensic certifications –

		individual resources having any of the additional Professional Forensic certifications – CCFE (Certified Computer Forensic Examiner), CCE (Certified Computer Examiner), CHFI (Computer Hacking & Forensic Investigator) - (Copies of Certificates of all the resources and their resume with details on role/ jobs handled etc. for each of above certificates are to be submitted). Other certifications in Web App Penetration Testing and Ethical Hacking (Web Application Penetration Tester); Wireless Ethical Hacking, Penetration Testing and Defense (Assessing Wireless Network); Advanced Penetration Testing, Exploits and Ethical Hacking (Exploit Researcher and Advanced Penetration Tester) are desirable. The Bidder is required to provide at least 5 indicative resumes/CVs of the prospective project team members having qualifications /certifications /experience as mentioned above.	professional-12 minimum 10 resources with minimum 5 years of experience in IT Security domain/Digital Cyber Forensics having any of the following certifications - CISA / CISSP /CEH/CISM & Minimum two resources with any one of the below certificate CCFE (Certified Computer Forensic Examiner)/ CCE (Certified Computer Examiner)/ CHFI (Computer Hacking & Forensic Investigator) .	CCFE (Certified Computer Forensic Examiner), CCE (Certified Computer Examiner), CHFI (Computer Hacking & Forensic Investigator). The Bidder is required to provide at least 5 indicative resumes/CVs of the prospective project team members having qualifications /certifications /experience as mentioned above.
20	8.8	✓ Applicant or their subsidiaries/sister concerns whose Partner /Director is a member of the Bank's Board.	Request you to remove this clause as Non-Disclosure agreement would be placed in between bank & the auditor organization. Being an auditor there will be no conflict of interest that can emerge as there	Please adhere to the RFP terms & conditions

		✓ Who have undertaken IS Audit of the Bank presently or in the last one year as on 31.03.2021.shall not be eligible to participate in the RFP	will be NDA for sharing the information between the auditor & auditee .Also, we are Govt of India empanelled organization. Thus we request you to kindly remove this clause.	
21	8.11	To ensure independence, the Bidder should not be a System Integrator for Network/SOC/CBS for the Bank IT Infrastructure either presently or for the last one year as on 31.03.2021..	Request you to remove this clause as Non-Disclosure agreement would be placed in between bank & the auditor organization. Being an auditor there will be no conflict of interest that can emerge as there will be NDA for sharing the information between the auditor & auditee. Also, we are Govt. of India empanelled organization. Thus we request you to kindly remove this clause.	Please adhere to the RFP terms & conditions
22	8 (5)	The Prospective team should have minimum 10 resources with minimum 5 years of experience in IT Security domain/Digital Cyber Forensics having any of the following certifications - CISA / CISSP /CEH/ CISM with at least 2 individual resources having any of the additional Professional Forensic certifications – CCFE (Certified Computer Forensic Examiner), CCE (Certified Computer Examiner), CHFI (Computer Hacking & Forensic Investigator)	Besides the forensic certification required for at least 2 individual resources we request you to add CFE (Certified Fraud Examiner) which is renowned certification worldwide.	CFE (Certified Fraud Examiner) may be considered for resource qualification criteria

23	8 (8)	Applicant or their subsidiaries/sister concerns • whose Partner/Director is a member of the Bank's Board. • who have undertaken IS Audit of the Bank presently or in the last one year as on 31.03.2021. shall not be eligible to participate in the RFP	We feel it is irrelevant who were the IS Auditor in the last one year as on 31-03-2021 and the same should be deleted. We required you to modify the 2nd part of this clause as under: "who have undertaken IS Audit of the Bank presently"	Please adhere to the RFP terms & conditions
24	8 (9)	The Bidder should have provided Digital/Cyber forensic analysis services for at least Five (5) BFSI/Public/Private organizations during the last five years.	We request you to modify the clause as under: "The Bidder should have provided Digital/Cyber forensic analysis services for at least Three (3) BFSI/Public/Private organizations during the last five years.	Please adhere to the RFP terms & conditions
25		The appointed vendor shall be enrolled to conduct a desktop exercise at the time of appointment to throw light on the first and vital steps to be taken up at the time of any incident with all the related	Kindly furnish the total number of participants and location. Will the exercise be a onetime activity	This will be a onetime activity in the form of a kick-off meeting to be held at Head Office, ISSD deptt. at the initiation of the Forensic Readiness Assessment Project /Start of on-demand forensic investigation services when an incident is reported.

26		As a part of the assessment of the Digital/Cyber Forensic Readiness of the Bank , the Auditor after review of the existing Infrastructure of the Bank has to provide an assurance / confirmation to the bank that Functioning of the Bank's IT system is in Compliance with – • Bank's IT Security Policy. • Bank's Cyber Security Policy./Cyber Crisis Management Plan RBI Information Security guidelines, Cert-In guidelines, any other legal requirements.	We understand the compliances against the policy mentioned is with reference to the scope of work only. Whether auditor need to verify the implementation/compliance of Bank's security policy and Cyber Security Policy/Cyber Crisis Management Plan	Please adhere to the RFP terms
27		Provide training /awareness to Bank's designated personnel in the area of Digital/ Cyber Forensic Investigation & related topics	Kindly furnish the total no. of participants and location. will it be one time exercise	Tentatively a team of 10 -15 members. The location will be at Chennai
28			Can the audit be performed through offsite location including training and desktop exercise	Forensic Audit shall be performed on-site at the Site of incidence and other related places as required for investigation purpose.
29			Total no. of applications/ infrastructure to be covered under Forensic Readiness Assessment/Incident Audit	Bank's IT infrastructure-Major items like CBS, Delivery Channels (ATMs, IB, MB, UPI etc.), Aadhar Enabled Payment system,

				SWIFT, IMPS, RTGS , NEFT etc among others. List of critical applications will be provided during the assessment time.
30			Whether Bank has Security Operation Centre in place and all the assets are integrated with SOC solution	Yes