UCO BANK
Department of Information Technology
Expression of Interest (EOI)
for
Empanelment of partners to carry out Forensic audit, Incident investigation for the Bank (E-tendering)
EOI Ref. No: UCO/DIT/601/2026-27 Date: 03-07-2026
Pre-Bid Responses/ Clarifications published on 29-07-2026

#	Bid Page No.	Bid Clause No.	Original Clause	Query sought/ Suggestions of the Bidder	Bank's Response
01	14	Part II – 1 (SCOPE OF AUDIT WORK)	Evidence collection must start immediately after request received for Digital Forensic Audit for Cyber –attack or any other cyber incident.	Kindly specify the expected response time (e.g., 2 hours, 4 hours, 8 hours, 24 hours) for mobilization of the forensic team after notification of an incident.	The selected bidder to ensure commencement of forensic audit activities within **4 hours** of intimation for incidents reported at the Bank's Primary Data Centre (DC) and Disaster Recovery (DR) sites. For incidents at all other Bank locations, forensic audit activities should commence within one week from the date of intimation or as accepted by the Bank, depending on the nature, criticality and location of the incident.
02	14	Part II – 1 (SCOPE OF AUDIT WORK	Evidence collection must start immediately after request received for Digital Forensic Audit for Cyber –attack or any	Kindly share a rough, location-wise estimate (Head Office/Data Centre/DR Site/Branches, etc.) of the number of cyber incidents investigated in the last three	The requested information pertains to the Bank's internal security operations and incident management records and is confidential in nature.

			other cyber incident.	years, to allow bidders to plan onsite/offsite deployment, travel and response-time costs.	
03	14	Part II – 1 (SCOPE OF AUDIT WORK	Evidence collection must start immediately after request received for Digital Forensic Audit for Cyber –attack or any other cyber incident.	Please suggest whether overseas locations are expected to be covered and would initial remote support be allowed? It is requested that information in this regard will be helpful in making arrangements with our counterparts in those countries.	The scope of the RFP is for Bank's servers, systems and infrastructure located within India. However, if technically feasible and appropriate, initial forensic activities that can be performed remotely shall be undertaken as part of the scope of work for overseas branches.
04	14	Part II – 1 (SCOPE OF AUDIT WORK)	Assist Bank's Incident Response Team to avoid delays and contamination.	Kindly confirm whether remote forensic investigation and evidence collection shall be permitted wherever technically feasible.	Remote forensic investigation and evidence collection may be permitted from the Bank's premises, wherever technically feasible, solely at the discretion of the Bank, based on the nature, criticality, and circumstances of the incident. The selected bidder shall be prepared to undertake onsite forensic investigation whenever required by the Bank. Such efforts will be finalized separately.
05	13	Part II – 1 (SCOPE OF AUDIT WORK)	Store evidence in tamper-proof systems or encrypted containers.	Kindly confirm if the storage media be provided and stored by the bank or be used and stored by bidder.	The required storage media shall be provided by the Bank on demand.
06	13	Part II – 1 (SCOPE OF AUDIT WORK)	All digital evidence must be accompanied by a Section 65B Certificate to ensure legal admissibility in Indian courts.	With the enforcement of the **Bharatiya Sakshya Adhiniyam, 2023 (BSA, 2023)** replacing the **Indian Evidence Act, 1872**, one of the most crucial and frequently litigated provisions — **Section 65B**, dealing with the	Please refer corrigendum.

				admissibility of electronic records — has been re-enacted in a modified form as **Section 63(4)(c)**. So, kindly request bank to change the clause accordingly. Kindly confirm whether the Bidder's forensic expert is required to personally appear before courts/law-enforcement agencies, such attendance/deposition is chargeable separately or deemed included in scope.	
07	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	To assess preparedness to effectively investigate incidents such as internal and external fraud, technology and system failures, cyber incidents including data breaches, insider threats, system abuse and third-party vendor-related cyber incidents.	Please confirm whether the forensic readiness assessment covers the entire Bank, including Head Office, Data Centres, DR Site, Cloud infrastructure, Branches, ATMs, and subsidiaries, or only the IT infrastructure managed by the Bank	The scope of the forensic readiness assessment shall be determined by the Bank based on the specific engagement. Relevant details pertaining to the systems, infrastructure, locations and entities to be covered shall be shared with the successful bidder, wherever applicable and required for execution of the assignment.
08	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Analysis of the existing infrastructure of the Bank along with regulatory guidelines w.r.t. enhancement of forensic readiness.	Kindly provide the approximate number of servers, endpoints, network devices, security devices, databases, applications, cloud workloads etc that are in scope.	The scope of the assessment shall be communicated by the Bank based on the specific engagement. Relevant details, wherever applicable and necessary for execution of the assignment, shall be shared with the successful bidder.
09	14	Part II - 2.	Analysis of the existing	Please specify the number of	The number of locations to be covered

		Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	infrastructure of the Bank along with regulatory guidelines w.r.t. enhancement of forensic readiness.	physical locations to be assessed and whether onsite visits are mandatory.	and the requirement for onsite visits shall depend on the specific engagement and the Bank's requirements. Relevant details, wherever applicable, shall be shared with the successful bidder. The selected bidder shall be prepared to undertake onsite visits whenever required by the Bank.
10	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Analysis of the existing infrastructure of the Bank along with regulatory guidelines w.r.t. enhancement of forensic readiness.	Has the Bank previously conducted a forensic readiness assessment? If yes, will previously reports and remediation status be shared?	The information sought pertains to the Bank's internal security assessments and is confidential in nature. Relevant details, wherever applicable and required for execution of the assignment, shall be shared with the successful bidder.
11	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Analysis and suggest appropriate security technologies and ensuring that security tools are properly integrated into existing systems.	Is the bidder expected to validate existing security tool integrations through technical testing or only through documentation review?	The selected bidder shall validate the existing security tool integrations through both technical verification/testing, wherever feasible and permitted by the Bank, and documentation review, as required for the scope of the engagement.
12	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Analysis and suggest appropriate security technologies and ensuring that security tools are properly integrated into existing systems.	Kindly provide the list of security tools currently deployed (SIEM, EDR, SOAR, DLP, PAM, IAM, Email Security, Proxy, Firewall, WAF, UEBA, CASB, etc.).	The requested information pertains to the Bank's information security architecture and is confidential in nature. Relevant details, wherever applicable and required for execution of the assignment, shall be shared with the successful bidder.
13	14	Part II - 2. Forensic Readiness for cyber-attack	Analysis and suggest appropriate security technologies and ensuring that security	Please provide the list of log sources integrated with the SIEM along with log retention periods	The requested information pertains to the Bank's security monitoring infrastructure and log management practices and is confidential in nature.

		or any other cyber incident (Half Yearly):	tools are properly integrated into existing systems.		Relevant details, wherever applicable and required for execution of the assignment, shall be shared with the successful bidder.
14	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Analysis of the existing infrastructure of the Bank along with regulatory guidelines w.r.t. enhancement of forensic readiness.	Does the Bank use AWS, Azure, GCP, or any private cloud? If yes, please provide the approximate number of subscriptions/accounts/projects in scope.	The requested information pertains to the Bank's IT infrastructure and cloud environment and is confidential in nature. Relevant details, wherever applicable and necessary for execution of the assignment, shall be shared with the successful bidder.
15	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	To assess preparedness to effectively investigate incidents such as internal and external fraud, technology and system failures, cyber incidents including data breaches, insider threats, system abuse and third-party vendor-related cyber incidents.	Are third-party hosted applications and managed services included in the scope? If yes, please specify the number of vendors.	Yes. Third-party hosted applications and managed services, wherever applicable, are included within the scope of the engagement. However, the details and number of such vendors are confidential and shall be shared with the successful bidder, wherever relevant and required for execution of the assignment
16	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Review Secure Configuration Documents adopting best practices for servers OS, Web application, Database, Security Devices, Network Devices etc.	Please specify the approximate number of operating systems, databases, web applications, security devices, and network devices whose secure configurations need to be reviewed.	The requested information pertains to the Bank's IT infrastructure and is confidential in nature. The scope of review shall be determined by the Bank based on the specific engagement. Relevant details, wherever applicable and required for execution of the assignment, shall be shared with the successful bidder.
17	14	Part II - 2. Forensic Readiness for	Analysis of the existing infrastructure of the Bank along with regulatory	Does the infrastructure analysis include architecture review only, or is configuration validation also	The scope of infrastructure analysis shall include both architecture review and configuration validation, wherever

		cyber-attack or any other cyber incident (Half Yearly):	guidelines w.r.t. enhancement of forensic readiness.	expected?	applicable and as required for the specific engagement. The methodology shall be finalized in consultation with the Bank.
18	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Conducting simulated forensic drill and tabletop exercises on a half-yearly basis to validate the institution"s readiness to handle cyber incidents and ensure effective evidence collection, preservation, and analysis in line with regulatory expectations.	Kindly clarify the scope of the simulated forensic drill. Is it limited to a tabletop exercise, or does it include live technical evidence acquisition and forensic investigation?	The scope of the simulated forensic drill shall include both tabletop exercises and live technical evidence acquisition and forensic investigation, wherever applicable. The detailed scope, objectives, and scenarios for each drill shall be finalized by the Bank in consultation with the selected bidder.
19	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	To assess the ability to collect, preserve and analyze digital evidence in a legally admissible manner, thereby strengthening the bank"s forensic posture.	Will the Bank provide remote access to systems and documents, or will the assessment require onsite presence?	The assessment shall be carried out through onsite presence at the Bank's designated location(s).
20	14	Part II - 2. Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	To assess the ability to collect, preserve and analyze digital evidence in a legally admissible manner, thereby strengthening the bank"s forensic posture.	Will the Bank provide the SOP to be followed for the collection, preservation and analysis of digital evidence or should the SOP of the bidder be utilized.	The Bank's existing SOPs, policies, and procedures shall be made available to the successful bidder before engagement of the assignment.
21	14	Part II - 2. Forensic Readiness for cyber-attack or any other	Identifying weaknesses in a Bank's security posture.	Please confirm whether the security posture assessment covers the entire Bank, including Head Office, Data Centres, DR Site, Cloud infrastructure,	The security posture assessment shall cover the Bank's overall IT environment, including, wherever applicable, Head Office, Data Centres, Disaster Recovery (DR) Site, Cloud infrastructure,

		cyber incident (Half Yearly):		Branches, ATMs, and subsidiaries, or only the IT infrastructure managed by the Bank	Branches, ATMs, other relevant IT assets and infrastructure including third party sites associated with the Bank. The assessment shall specifically include evaluation of log generation, log collection, log retention, log utilization and identification of deficiencies in logging, monitoring or availability of forensic artifacts necessary for effective incident investigation and forensic analysis. The detailed scope of each engagement shall be communicated by the Bank at the time of assignment.
22	14	Part II – 3. Personnel Expertise	Auditor should possess adequate expertise in digital forensics and be responsible for enhancing the capability of bank staff in various aspects of forensic readiness by providing training.	Please confirm the estimated count of bank staff to be trained on digital forensics aspects. Please specify the mode of training (offline/online)	The number of participants and the mode of training (online, offline, or hybrid) shall be decided by the Bank based on its requirements for the specific engagement. Relevant details shall be shared with the successful bidder.
23	09	PART I -3. Eligibility Criteria	The bidder must be having Two (2) professionals who hold professional certifications like CFE (Certified Fraud Examiner) or FAFD (Forensic Accounting and Fraud Detection) with requisite experience to handle the work as per the scope (valid as on bid submission date).	Kindly confirm if financial fraud audit is required or not, as it is not a part of scope of work specified in the tender document	Clause is self-explanatory
24	09	PART I -3.	The bidder should have	Request the Bank to define	For the purpose of this RFP, "Cyber

		Eligibility Criteria	done minimum 5 Cyber forensic audits for different type of incidents in single or multiple organization during last 3 years as on bid submission date. Out of which one shall be in Schedule commercial Bank in India.	'Cyber forensic audit' for the purpose of this eligibility criterion – i.e., whether it includes incident investigation, malware analysis, data breach investigation, and fraud investigation assignments, or is restricted to formal forensic audits only. Also clarify whether audits performed for NBFCs, Cooperative Banks, Payment Banks or other BFSI/regulated entities (other than a Schedule Commercial Bank) will be counted towards the remaining 4 of the 5 required audits.	Forensic Audit" includes digital forensic investigations relating to cyber incidents such as malware analysis, ransomware incidents, data breach investigations, insider attack investigations, cyber fraud investigations, incident response engagements and other cyber incident investigations involving forensic evidence collection, preservation, analysis, and reporting. Out of the minimum five (5) qualifying assignments, at least one (1) must have been successfully executed for a Scheduled Commercial Bank in India. The remaining assignments may have been carried out for Government Organizations, Public Sector Undertakings (PSUs), Scheduled Commercial Banks, NBFCs, Cooperative Banks, Payment Banks, Insurance Companies, Financial Institutions or other regulated entities.
25	09	PART I -3. Eligibility Criteria	Documentary proof must be provided along with copies of Work Order OR completion certificate.	Kindly request the Bank to also consider the Engagement Letter or the Agreement executed between bidder and the Client as acceptable documentary proof.	Clause is self-explanatory.
26	86	Technical Specification	The bidder to have at least 10 no. of resources on its payroll having requisite experience of conducting any areas of	Kindly specify whether all 10 resources should have valid certificate at the time of bid submission.	Atleast ten (10) resources proposed by the bidder shall be on the bidder's payroll and shall possess valid certifications, as specified in the RFP, as on the bid submission date.

			the Audit as per the scope of EOI. The auditing team should be a mix of CISA /DISA /CISSP /CISM/CEH / ISO 27001 LA / GIAC Certified Forensic Analyst(GCFA)/ Certified Forensic Computer Examiner (CFCE)/ Computer Hacking Forensic Investigator(CHFI)/ Certified Computer Examiner(CCE)/Encase Certified Examiner (EmCE)/Digital Forensics Essentials(DFE) (Certificate to be valid as on bid submission date) required to conduct forensic audit as per the Scope.	Additionally, request bank to consider other certifications/ Master's Degree w.r.t. digital forensics/cyber security.	Please refer corrigendum/addendum
27	15	Part III: Contract Period	The tenure of the empanelment will be for a period of **3 (three) years** effective from the date of execution of the Service Level Agreement (SLA) unless terminated earlier by the Bank by serving 90 days" prior notice in writing to the selected bidder at its	Kindly note that this shall be subject to successful completion of our annual internal risk checks. Please let us know if it is acceptable.	Clause stands as per RFP.

			own convenience without assigning any reason and without any cost or compensation therefore.		
28	29	Part IV: 32. Liquidated Damage	Liquidated Damage Notwithstanding Bank's right to cancel the order, liquidated damages at 0.5% (half percent) of the price of the undelivered portion / non-installed hardware or service of the order value per week will be charged for each week's or part thereof of delay in the specified delivery/installation of services / hardware schedule subject to a maximum of 10% of the total cost of ownership. Bank will have right to recover these amounts by any mode such as adjusting from any payments to be made to the Vendor or from the performance Bank Guarantee. Liquidated damages will be calculated per week basis or part thereof of delay. Dispatch details	We request the Bank to kindly clarify and amend the LD clause to specify that Liquidated Damages shall be applicable only for delays solely and directly attributable to the successful bidder. Since project execution and delivery milestones are dependent upon timely availability of information, approvals, access, infrastructure readiness, decisions, and other support from the Bank and/or its designated third parties, any delays arising from such dependencies should be excluded from LD computation. Further, LD, if applicable, should be calculated only on the value of the delayed deliverable/item and not on the overall contract/TCO value. Applicable LDs - rate of 1% of the order value of the late delivered item for each week"s delay or part thereof, subject to maximum of 10% of value of the late delivered items.	Clause stands as per RFP.

			shall be shared by the vendor regularly after handing over the consignment to the concerned Courier Agency/Indian Postal services.		
29	33	Part IV: 39. Confidentiality and Secrecy	The selected service provider shall ensure that the same is not used or permitted to be used in any manner incompatible or inconsistent with that authorized by the UCO Bank. The Confidential Information will be safeguarded and the selected service provider will take all necessary action to protect it against misuse, loss, destruction, alterations or deletions thereof.	The confidentiality obligations are open-ended. We request that confidentiality obligations survive for a finite period of one (1) year from expiry/termination of the engagement or relevant work order, except to the extent otherwise required by applicable law.	Please refer corrigendum.
30	33	Part IV: 40: Compliance with Law	The Vendor shall undertake to observe, adhere to, abide by, comply with and notify the Bank about all laws in force or as are or as made applicable in	We request deletion of broad indemnity obligations and clarification that the bidder's obligations shall be limited to compliance with applicable laws relevant to the services being provided under the	Clause stands as per RFP.

			future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this Contract and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees/officers/staff/ personnel/ representatives/ agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may Occurs or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising therefrom.	engagement.	
31	33	Part IV: 40: Compliance with Law	All the employees/operator deployed by the Vendor for the digitization activity must comply with government‟s rules and regulations like Minimum Wages Act, Provident Fund, Labour Law, ESIC	Kindly clarify that obligations under this clause apply solely to the bidder entity and not personally to its employees, officers or personnel.	Clause stands as per RFP.

			facility standard, CVC / RBI guidelines.		
33	49	Part IV: 66: Compliance with is/cyber security policy	The selected bidder shall have to comply with Bank"s IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the selected Bidders	We request clarification as we have internal security policies of our own and if required bank will have to request the bidder in advance, subject to review and acceptance by the bidder.	Clause stands as per RFP.
34	50	Part IV: 67: Compliance With Reserve Bank of India's Outsourcing Policy 2025	During bid submission bidders should ensure compliance with the RBI"s circular on "Commercial Banks- Managing risk in outsourcing directions, 2025" vide circular no. RBI/DOR/2025-26/171, DOR.ORG.REC.No. 90/21-04-158/2025-26 dated November, 28 2025. Selected bidder should comply with the directions of above referred RBI circular post award of contract. The selected bidder must comply with Bank"s outsourcing policy and must undergo due diligence process described in the policy. The necessary questioner and report formats shall	Kindly clarify this as this is only applicable to the bank.	Clause stands as per RFP.

			be shared with the selected bidder.		
35	50	Part IV: 69: Non-Assignment	The Vendor agrees that the Vendor shall not be entitled to assign any or all of its rights and or obligations under this Agreement to any entity including the Vendor"s affiliate without the prior written consent of the Bank. If the Bank undergoes a merger, amalgamation, take-over, consolidation, reconstruction, change of ownership, etc., this Agreement/Contract shall be considered to be assigned to the new entity and such an act shall not affect the rights of the Vendor under this Agreement/Contract.	We request that the assignment restriction be made mutual, such that neither party may assign its rights or obligations without the prior written consent of the other party, except in connection with mergers, restructuring or internal reorganizations.	Clause stands as per RFP.
36	58	Part IV: 79: No Rights to Set-Off	In case the Vendor has any other business relationship with the Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available to the Vendor under this arrangement with the Bank for any payment	Kindly request bank to remove this clause	Clause stands as per RFP

			receivable under and in accordance with that business.		

UCO BANK
Department of Information Technology
Empanelment of partners to carry out Forensic audit, Incident investigation for the Bank (E-tendering)
EOI Ref. No: UCO/DIT/601/2026-27 Date: 03-07-2026
Corrigendum/Addendum published on 29-07-2026

Sl. No	RFP Page No.	Original Clause	Modified Clause
1.		**New Clause added in PART II Scope of Audit Work**	**The Scope of work is indicative. The quotations may be invited based on the prevailing scenario.**
2.		**New Clause added in PART II Scope of Audit Work:** **Cooling Period**	IS Audit Firms who were engaged earlier with the Bank and completed their contract period, will have a cooling period of 2 years after expiry of their contract period. Hence, such bidders need not to apply for the Bid. Further, this cooling period will not be applicable for Audit firms who were engaged to carry out any Special Audit(s) through a separate selection process.

3.	Bid submission date	Last Date and Time for receipts of tender bids : 04/08/2026 at 04:00 PM Opening of Technical Bids : 04/08/2026 at 04:30 PM	Last Date and Time for receipts of tender bids : **07/08/2026** at 04:00 PM Opening of Technical Bids : **07/08/2026 at 04:30 PM**
4.	Page 14 2.Forensic Readiness for cyber-attack or any other cyber incident (Half Yearly):	Conducting simulated forensic drill and table top exercises on a half-yearly basis to validate the institution's readiness to handle cyber incidents and ensure effective evidence collection, preservation, and analysis in line with regulatory expectations.	Conducting simulated forensic drill and table top exercises on a **Quarterly** basis to validate the institution's readiness to handle cyber incidents and ensure effective evidence collection, preservation, and analysis in line with regulatory expectations. Drill scenario may be changed considering emerging threats and risks during the contract period, that too also if so warranted.
5.	Page 15,16 STAGES OF EVALUATION	There would be two (2) stages for evaluation process. The Stages are: Eligibility Criteria Evaluation Technical Evaluation The Eligibility Criteria would be evaluated first for the participating bidders. The bidders, who qualify all Eligibility Criteria as mentioned above, will be shortlisted for the technical bid evaluation. A detailed technical evaluation would be undertaken for eligible bidders and only the technically qualified bidders would be	There would be two (2) stages for evaluation process. The Stages are: Eligibility Criteria Evaluation Technical Evaluation The Eligibility Criteria would be evaluated first for the participating bidders. The bidders, who qualify all Eligibility Criteria as mentioned above, will be shortlisted for the technical bid evaluation. A detailed technical evaluation would be undertaken for eligible bidders and only the technically qualified bidders would be shortlisted

		shortlisted for empanelment (Minimum 3 and Maximum 5).	for empanelment (Minimum 3 and Maximum 5). **The Bank at its own discretion may reduce the minimum number of empanelled partners to 2 (two).**
6.	Part II – 1 (SCOPE OF AUDIT WORK)	All digital evidence must be accompanied by a Section 65B Certificate to ensure legal admissibility in Indian courts.	All digital evidence must be accompanied by the certificates, declarations and documentation as applicable under the prevailing laws of India, to ensure its legal admissibility before the competent authorities/courts. Further, if the services of the bidder's forensic expert are required for appearance before courts, law enforcement agencies or other competent authorities in connection with the forensic investigation, the same shall form part of the scope of work and no additional charges shall be payable unless otherwise specifically agreed by the Bank.
7.	Part IV: 39. Confidentiality and Secrecy	The selected service provider shall ensure that the same is not used or permitted to be used in any manner incompatible or inconsistent with that authorized by the UCO Bank. The Confidential Information will be safeguarded and the selected service provider will take all necessary action to protect it against misuse, loss, destruction, alterations or deletions thereof.	The selected service provider shall ensure that the same is not used or permitted to be used in any manner incompatible or inconsistent with that authorized by the UCO Bank. The Confidential Information will be safeguarded and the selected service provider will take all necessary action to protect it against misuse, loss, destruction, alterations or deletions thereof. **The confidentiality obligations survive for a period of two (2) years from expiry/termination of the engagement or relevant work order, except to the extent otherwise required by applicable law. The bidder has to provide a termination Certificate at**

			the time of expiry of two (2) years mentioning the selected service provider will take all necessary action to protect it against misuse, loss, destruction, alterations or deletions thereof.
8.	Page 9 3.ELIGIBILITY CRITERIA	The bidder must be having on their rolls, on permanent employment basis, a minimum of 10 (ten nos.) professionals who hold professional certifications like CEH/CISA / CISSP / CISM / ISO 27001 LA / DISA (ICAI)/GIAC Certified Forensic Analyst(GCFA)/ Certified Forensic Computer Examiner (CFCE)/ Computer Hacking Forensic Investigator(CHFI)/ Certified Computer Examiner(CCE)/Encase Certified Examiner(EmCE)/Digital Forensics Essentials(DFE) with requisite experience to handle the work as per the scope (valid as on bid submission date).	The bidder must be having on their rolls, on permanent employment basis, a minimum of 10 (ten nos.) professionals who hold professional certifications like CEH/CISA / CISSP / CISM / ISO 27001 LA / DISA (ICAI)/GIAC Certified Forensic Analyst(GCFA)/ Certified Forensic Computer Examiner (CFCE)/ Computer Hacking Forensic Investigator(CHFI)/ Certified Computer Examiner(CCE)/Encase Certified Examiner(EmCE)/Digital Forensics Essentials(DFE)/ **Post Graduate degree in digital forensics** with requisite experience to handle the work as per the scope (valid as on bid submission date).

REVISED ANNEXURE- XV

Sl. No	Evaluation Parameters	Max Marks	Scoring Methodology	Score
A.	Average turnover in last 3 years	10	• 10 Marks – More than 10 Cr • 7.5 marks – >5 Cr and up to 10 Cr • 5 marks – 5 Cr	
B.	The bidder should have experience in the field of cyber forensic Audit and digital forensics in any Schedule commercial Bank in India as of bid submission date.	15	• 15 marks – More than 5 years of experience. • 10 marks – >3years and up to 5 years of experience. • 08 marks – 3 years of experience.	
C.	The bidder should have carried out Cyber forensic audits for different type of incidents in single or multiple organizations during past 3 years.	10	• Additional one mark for Forensic Audit beyond 5 maximum 10 marks • 05 marks – 5 cyber forensic audits	
D.	The bidder must have no. of professionals on their rolls, on permanent employment basis who hold professional certifications like CEH/CISA / CISSP / CISM / ISO 27001 LA / DISA (ICAI)/GIAC Certified Forensic Analyst(GCFA)/ Certified Forensic Computer Examiner (CFCE)/ Computer Hacking Forensic Investigator(CHFI)/ Certified Computer Examiner(CCE)/Encase Certified Examiner(EmCE)/Digital Forensics Essentials(DFE)/ **Post Graduate degree in digital forensics** with requisite experience to handle the work as per the scope (valid as on bid submission date).	15	• 15 marks – 15 or more professionals. • 10 marks – 11 to 14 professionals. • 08 marks – 10 professionals.	

E.	No. of digital forensic specialists in the Firm. Copies of certification/Degree in CFE (Certified Fraud Examiner) or FAFD (Forensic Accounting and Fraud Detection) etc. related Certificate in Forensic Audit.	15	• 15 Marks – More than 5 digital forensic Specialists • 10 Marks – 3-5 digital forensic Specialists • 8 Marks - 2 digital forensic Specialists	
F.	The bidder should have conducted Forensic Audit in following areas: 1. Computer forensic Audit 2. Mobile device Forensic Audit 3. Network Forensic Audit 4. E-mail and social media forensic audit 5. Database Forensic Audit	35	7 (seven) Marks for each type of audit for different incidents/purpose in single or multiple organization. The bidder has to submit both Purchase Order or Completion Certificate mentioning each type of audit	

(Please submit relevant documents for marks claimed)

Place:
Date:

AUTHORISED SIGNATORY
Name:
Designation:

All other terms and conditions of the above bid document will remain unchanged.