केनरा बैंक Canara Bank

Pre bid queries replies for GeM bid ref.no.GEM/2024/B/4996850 dated 31/05/2024 for Engagement of Auditor for Conducting Comprehensive Cybersecurity Audit of CBS and other Critical Infrastructure through a CERT -In Empaneled Auditor

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1	12	SECTION B - INTRODUCTION	9.Scope of Work	9.4.The selected Bidder should have pool of at least twenty (20 Nos) professionals, to deploy on site, in case if required for conducting the assessment, with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment.	Request clarification whether the pool of resources mentioned are on need-basis (as and when if required) or the bidder requires to factor the estimation for count of 20 professionals to be dedicated for the project. Also please clarify the details of the relevant qualifications mentioned in the clause.	Details of relevant qualifications are mentioned in Annexure-10.
2	12	SECTION B - INTRODUCTION	10.Project Completion and Management	10.1.1.For smooth completion of project, the selected Bidder should identify one or two of its representatives at Bengaluru as a single point of contact for the Bank.	Please clarify whether the personnel is required to be present on-site at the Banks premises or the professional can operate remotely from any location within Bangalore or outside.	Bidder to comply with the RFP terms and Conditions. The selected bidder should have the resources available at bengaluru as SPOC for the bank.
3	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.Project Timelines	1.2The entire assessments for Cyber Security Audit of CBS & Other Critical Infrastructure have to be completed within 7 Months from the date of acceptance of Purchase Order or within 7 months and 1 week from the date of issuance of Purchase Order. Audit may be extended if any bank dependency arises.	Please clarify regarding the contract period and timelines of the project. As per GeM document the assignment is for a period of 08 months whereas here it is mentioned as 07 months.	Bidder to comply with the RFP terms and conditions.
4	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.5The timelines for the projects will be as under:	Phase 1 Revalidation Assessment: Completion of verification for Critical and High Risk observations.1 Month from date of completion of closure of Observations of Initial Assessment of Phase-1.	Request clarificartion on the timeline for completion of closure of observations. We understand that Bank shall undertake the responsibility for closure of all observations.	Bidder to comply with the RFP terms and conditions.
5	14	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.5The timelines for the projects will be as under:	Phase 2 Revalidation Assessment: Completion of verification for Critical and High Risk observations.2 Months from date of completion of closure of the Observations of Initial Assessment of Phase 2.	Request clarificartion on the timeline for completion of closure of observations. We understand that Bank shall undertake the responsibility for closure of all observations.	Bidder to comply with the RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
6	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.Project Timelines	1.9If the Bidder fails to complete the assignment as per the time frame prescribed in the RFP, and the extensions if any allowed, it will be breach of contract. The Bank reserves its right to cancel the order in the event of delay and invoke the Bank Guarantee.	We understand that the bidder shall not be held responsible for any delay over which the bidder has no control or contribution.	Bidder to comply with the RFP terms and conditions.
7	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.Project Timelines	1.11Bank shall reserve the right to change the timelines in order to comply with regulatory guidelines without any additional cost.	We request to consider that any substantial change in the timeline may be considered for additional cost. Any reduction in timeline may also require to engage more manpower resources which may also conclude to additional cost.	Bidder to comply with the RFP terms and conditions.
8	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	2.Security	2.2.The selected Bidder will ensure the software delivered is in conformity with security standards and is without any security vulnerability.	We understand that the bidder shall not deliver any software for the Bank. Request to please ammend the clause.	The software which will be used for performing the assessment should be free from vulnerabilities and to comply with the latest security standards.
9	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	3.Penalties & Liquidated damages	3.1.Non-compliance of the Cyber Security Audit of CBS & Other Critical Infrastructure Assessment within the Phase wise timelines as per clause no.1.5 will result in imposing penalty of 0.50% on delay in the assessments per week or part thereof by the Bank on the total cost of audit for each phase mentioned in Annexure-14.	The bidder shall work at its best to meet the timline, considering that most of the requirements of the RFP have been fulfilled and timelines might be breached due to unforeseen circuymstances, we request to cap the liquidated damages penalty at 10% of the total project cost.	Bidder to comply with the RFP terms and Conditions.
10	18	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5.Documents, Standard Operating Procedures and Manuals	5.1.All related documents, manuals, Standard Operating Procedures (SOPs), best practice documents and information furnished by the Bidder shall become the property of the Bank.	We understand that the bidder shall not be responsible for preparation of any document or SOP. Please confirm and request to ammend the clause.	Bidder to comply with the RFP terms and Conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
11	18	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5.Documents, Standard Operating Procedures and Manuals	5.2.Provide comprehensive documentation of the application including but not limited to, the application architecture, description of the interfaces, the data model, database table structure, data flow diagrams, complete description of the data elements (metadata), user manual for all stakeholders (marketing team, operations teams) with step-by-step process and workflow with screenshots and any such requirements of the bank	We understand that the bidder shall not be responsible for preparation of any document related to application or database or any matter mentioned in the clause. Please confirm and request to ammend the clause.	Bidder to comply with the RFP terms and Conditions.
12	18	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	7.Right to Audit	7.1.The selected Bidder (Service Provider) has to get itself annually audited by internal/external empaneled Auditors appointed by the Bank/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank/such auditors in the areas of products (IT hardware/software) and services etc., provided to the Bank and the Service Provider is required to submit such certification by such Auditors to the Bank. The Service Provider and or his/their outsourced agents/subcontractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the Service Provider. The Service Provider shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. Corresponding clauses 7.2 and 7.3	The bidder shall already have an competant authority in place for the audit of its systems. The clause may pose as a restrictive clause and request to omit the clause.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
13	24	SECTION D - BID PROCESS	7.Software Version	The Bidder should ensure usage of latest licensed software with proper update/patches and their subcomponents as has been sought in the technical/functional requirements. The Offer may not be evaluated and / or will be liable for rejection in case of non-submission or partial submission of Software Version of the items offered. Please note that substituting required information by just software name is not enough. Bidder should not quote Software which is already End of Sale. Bidder also should not quote Software which are impending End of Sale.	We understand that the bidder shall not be supplying any software product as the assignment is for Cyber Security Assessment. Request to consider and ammend the clause.	The software which will be used for performing the assessment should be free from vulnerabilities and to comply with the latest security standards.
14	24	SECTION D - BID PROCESS	8.Documentation	Technical information in the form of Brochures / Manuals / CD etc. of the most current and updated version available in English must be submitted in support of the Technical Offer made without any additional charges to the bank. The Bank is at liberty to reproduce all the documents and printed materials furnished by the Bidder in relation to the RFP for its own use.	We understand that the assignment / project is service based and does not contain any product. Hence, the technical information in the modes asked may not be submitted. Request to consider and ammend the clause.	Bidder to comply with the RFP terms and Conditions.
15	24	SECTION D - BID PROCESS	11.Assumptions/Presumptions/Modifications	The Bank would like to expressly state that any assumption, presumptions, modifications, terms, conditions, deviation etc., which the Bidder includes in any part of the Bidder's response to this RFP, will not be taken into account either for the purpose of evaluation or at a later stage, unless such assumptions, presumptions, modifications, terms, conditions deviations etc., have been accepted by the Bank and communicated to the Bidder in writing. The Bidder at a later date cannot make any plea of having specified any assumption, terms, conditions, deviation etc., in the Bidder's response to this RFP document. No offer can be modified or withdrawn by a Bidder after submission of Bid/s.	We understand there might be certain requirement fo which clarity may be given on winning the opoortunity and the bidder may proceed for the proposal with assumptions. Request to consider such assumptions which does not alter the purpose and requirement of the project.	Bidder to comply with the RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
16	25	SECTION D - BID PROCESS	12.Submission of Bids	12.1.The Bidder has to submit their response in GeM portal before the bid end date & time mentioned in the RFP document. The physical documents (viz., EMD, Integrity Pact etc.,) should be submitted to the below mentioned officials before the bid end date & time at the Venue specified in the Bid Schedule.	Request to provide at least 05 days time period for submission of hard copy considering the time taken for outstation parcel / courier.	Bidder to comply with the RFP terms and conditions.
17	27	SECTION D - BID PROCESS	4.Normalization of Bids	4.1.The Bank may go through a process of technical evaluation and normalization of the bids to the extent possible and feasible to ensure that, shortlisted Bidders are more or less on the same technical ground. After the normalization process, if the Bank feels that, any of the Bids needs to be normalized and that such normalization has a bearing on the price bids; the Bank may at its discretion request all the technically shortlisted Bidders to re-submit the technical and Commercial Bids once again for scrutiny.	Considering the criticality of the project, the technically qualified bidders may be selected for next phase of evaluation. Request to remove the clause.	Bidder to comply with the RFP terms and conditions.
18	35	SECTION G - GENERAL CONDITIONS	4.Human Resource Requirement	4.6.5.Background Police Verification report - Duly attested photocopy by candidate and bidder HR.	This clause may pose as a restrictive point. The bidder shall do due diligence during the on-boarding of the personnel under the payroll of the bidder. Declaration of the same may be provided by the authorized signatory or HR. Request to remove / ammend the clause.	Bidder to comply with the RFP terms and Conditions.
19	39	SECTION G - GENERAL CONDITIONS	12.Training and Handholding	12.5.Successful bidder shall hold technical knowledge transfer sessions with designated technical team of Business and/or any replacement Service Provider in at least last three (3) months of the project duration or as decided by Bank.	We understand that the period of three months mentioned is inclusive of the contract period. The bidder shall not be liable for any delay in the appointment of any party for knowledge transfer. Please confirm.	Bidder to comply with the RFP terms and Conditions.The bidder should be able to pass on the technical knowledge transfer session as decided by the bank over and above the assessment period.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
20	39	SECTION G - GENERAL CONDITIONS	14.Business Continuity Plan:	14.1.The service provider/vendor/ Bidder shall develop and establish a robust Business Continuity and Management of Disaster Recovery Plan if not already developed and established so as to ensure uninterrupted and continued services to the Bank and to ensure the agreed upon service level. 14.2.The service provider/vendor/ Bidder shall periodically test the Business Continuity and Management of Disaster Recovery Plan. The Bank may consider joint testing and recovery exercise with the Service provider/vendor.	We understand that development and testing of Business Continuity Plan should be the responsibility of the Bank or any implementation agency appointed by the Bank. The bidder shall be responsible for assessment and may assist in recommendations in case any gap observed in the documentation.	Bidder to comply with the RFP terms and conditions.
21	40	SECTION G - GENERAL CONDITIONS	16.Adherence to Banks IS Security/Cyber Security Policies:	16.2.In case of any security incident including but not limited to data breaches, denial of service, service unavailability, etc., the Bidder/vendor/Service Provider shall immediately report such incident to the Bank.	We understand that the bidder shall not be held liable for reporting of incidents. It should be the liability of the vendor / implementation agency appointed by the Bank. However, any incident if observed by the bidder shall be reported to the bank. Please confirm.	Bidder to comply with the RFP terms and Conditions.
22	53	Annexure-2 Pre-Qualification Criteria	Signing of Pre-Contract Integrity Pact	The bidder should submit signed Pre Contract integrity pact on Non Judicial Stamp Paper of Rs.500/- or more (as per respective state Stamp Act) as per Appendix-F.	We understand that in general INR 200 stamp paper is used for declarations and pacts. We request Bank to reassess and consider the value of the stamp paper.	Bidder to comply with the RFP terms and conditions.
23	53	Annexure-2 Pre-Qualification Criteria	Criteria	The Bidder should have minimum average annual turnover of Rs.1 crore from IT Security Audit Services for each year for the last three financial years (i.e., 2020-21, 2021-22 & 2022-23). This must be the individual company turnover and not of any group of companies.	Considering the criticality of the project, we request to consider **at least 50 crores turnover** for potentials bidder.	Bidder to comply with the RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
24	54	Annexure-2 Pre-Qualification Criteria	Criteria	The firm should have a pool of at least 20 professionals with active international accreditation like CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), CEH trained lead auditors employed with them.	We request to ammend the clause as: "The firm should have a pool of at least 20 professionals **with valid certification like CISA (Certified Information Systems Auditor) or CISM (Certified Information Systems Manager) or CISSP (Certified Information Systems Security Professional) or CEH or ISO 27001 LA** trained lead auditors employed with them."	Bidders to refer Corrigendum-1
25	55	Annexure-2 Pre-Qualification Criteria	1.Authorization Certificate - Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Power of Attorney or the Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.	We request to ammend the clause as: "**Bidder to submit a copy of the Power of Attorney or the Board Resolution evidencing the authority delegated to the authorized signatory**"	Bidder to comply with the RFP terms and conditions.
26	61	Annexure-7 List of Major Customers of the Bidder in Last 3 Years and References	Name, Designation, Telephone, Fax, Telex Nos., e-mail address of the contact person (customer)	.	Due to NDA signed and confidentiality clause, the bidder may not be able to share the client details. Request to consider and remove the client details section.	Bidder to comply with the RFP terms and conditions.
27	63	Annexure-9 Scope of Work	1.Comprehensive audit	a)web application (both thick client and thin client); b)mobile apps; c)APIs (including API whitelisting); d)databases; e)hosting infrastructure and obsolescence; f)cloud hosting platform and network infrastructure; and	Request to share the details and count of Applications, APIs, Databases, Infrastructure, etc. under the scope for better estimation of resources to be aligned to the project.	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
28	63, 64	Annexure-9 Scope of Work	1.Comprehensive audit	1.2.The scope of the comprehensive audit Should include, inter alia, the following: a), b), c), d), e), f), g).	Request to share the details and count of Applications, APIs, Databases, Infrastructure, etc. under the scope of review and assessment for better estimation of resources to be aligned to the project.	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
29	64	Annexure-9 Scope of Work	1.Comprehensive audit	1.2.The scope of the comprehensive audit Should include, inter alia, the following: k)security operations and monitoring review (including maintenance of security logs, correlation and analysis);	Request to share the details and count of the components present under the Security operations center. We understand that the bidder shall only review the operations and provide observations.	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
30	65	Annexure-9 Scope of Work	Deliverables and Report:	ISOG.3.1 1. Check for the information security and privacy certification of the audit entity / auditee organisation. Check valid ISO27001 certification at deployment location	Request to share the details of the locations or bank premises under the scope of the project.	Bangalore and Mumbai
31	72	Annexure-9 Scope of Work	Deliverables and Report:	A.4.2 2. Verify that the SAST tools are configured to check for compliance with coding standards and security policies.	Request to share the details of the tools utilized by Bank for SAST activity.	The details will be shared with the selected bidder
32	-	-	General query	-	Request to share the list of devices / equipments / assets / infrastructure under the scope of the bidder for assessment under the project.	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
33	97	Annexure-9 Scope of Work	Deliverables of Reports:	•PDF Excel, as well as two hard copies of reports, should be provided to the Bank after completion audit.	We request to consider that the bidder shall provide all reports in PDF format and through email only to maintain the integrity of the information shared.	Bidder to comply with RFP terms
34	98	Annexure-10 Technical Evaluation Criteria	Criteria	The Bidder should have conducted IT/ Information Security Risk Assessments, CBS assessment, IB and MB assessment, ATM Switch assessment, PCI-DSS assessment, Swift Assessment during the last five years i.e. 01/04/2019 to 31/03/2024 in BFSI sector organization/ Scheduled Commercial Banks/ Government Departments/ PSU organization in India.	We request to ammend the clause as: "The Bidder should have conducted **IT/ Information Security Risk Assessments / CBS assessment / IB and MB assessment / ATM Switch assessment / PCI-DSS assessment / Swift Assessment** during the last five years i.e. 01/04/2019 to 31/03/2024 in BFSI sector organization/ Scheduled Commercial Banks/ Government Departments/ PSU organization in India."	Bidders to refer Corrigendum-1

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
35	98	Annexure-10 Technical Evaluation Criteria	Criteria	The firm should have a pool of professionals with valid international accreditation like CISA (Certified Information Systems Auditor), CISM, CISSP (Certified Information Systems Security Professional), CEH and ISO 27001 trained lead auditors employed with them.	We request to ammend the clause as: "The firm should have a pool of professionals **with valid certification like CISA (Certified Information Systems Auditor) or CISM (Certified Information Systems Manager) or CISSP (Certified Information Systems Security Professional) or CEH or ISO 27001 LA** trained lead auditors employed with them."	Bidders to refer Corrigendum-1
36	98	Annexure-10 Technical Evaluation Criteria	Criteria	Copy of the certificates mentioned and letter from HR that stating they are on payroll of the bidder along with Date of joining. Note: Only those experiences will be counted which have duration of at least 1 year	Request to consider and remove: "Note: Only those experiences will be counted which have duration of at least 1 year"	Bidder to comply with the RFP terms and conditions.
37	-		General query	-	Considering the internal approval, review process and online payments, request to provide at least 15 working days for submission of proposal.	Bidder to comply with the RFP terms and conditions.
38	54	Annexure - 2 Pre-Qualification Criteria	8	The Bidder should have provided same Category of Assessment(s) in the last three Financial years before the bid opening date to any Central / State Govt Organization / PSU / Public Listed Company/BFSI sector.	How many such references are required? Whether the assessment relevant contracts / orders are required for each financial year?	Bidders to refer Corrigendum-1
39	98	Annexure-10 Technical Evaluation Criteria	a)	The Bidder should have conducted IT/ Information Security Risk Assessments, CBS assessment, IB and MB assessment, ATM Switch assessment, PCI-DSS assessment, Swift Assessment during the last five years i.e. 01/04/2019 to 31/03/2024 in BFSI sector organization/ Scheduled Commercial Banks/ Government Departments/ PSU organization in India.	We assume that the order copy along with work completion/undertaken proof or invoice can be submitted for any one of the activities - IT/ Information Security Risk Assessments or CBS assessment or IB and MB assessment or ATM Switch assessment or PCI-DSS assessment or Swift Assessment. Kindly confirm.	Bidders to refer Corrigendum-1
40	68	Annexure-9 Scope of Work	A	Source Code Assessment (SAST) Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's	Should the bidder perform the Source Code Assessment for all the in-scope applications/APIs?	Yes, bidder to comply with RFP terms

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
41	68	Annexure-9 Scope of Work	A	Source Code Assessment (SAST) Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's	What is the total count of applications (including web applications and mobile applications), API's inlcuding the CBS & Other Critical infra/Apps?	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
42	68	Annexure-9 Scope of Work	A	Source Code Assessment (SAST) Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's	How are the APIs hosted? Are you using any API Gateway? If yes, whether the configuration review of the API Gateway is also part of the scope?	The details will be shared with the selected bidder
43	71	Annexure-9 Scope of Work	A.4	Perform automated source code scan using a reliable open-source or proprietary scanning tool such as Fortify, SonarQube, Checkmarx etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis). Perform manual code review to identify the following vulnerabilities in the source code- sensitive information disclosure (including hard-coding of PII data, PII tokens, authentication tokens, security keys, encryption keys, passwords / user credentials, etc.)	Should the bidder perform the automated source code scan and manual code review or the bidder has to review the scan results only?	Bidder has to comply with RFP terms and to perform automated or manual scans as required
44	71	Annexure-9 Scope of Work	A.4	Perform automated source code scan using a reliable open-source or proprietary scanning tool such as Fortify, SonarQube, Checkmarx etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis). Perform manual code review to identify the following vulnerabilities in the source code- sensitive information disclosure (including hard-coding of PII data, PII tokens, authentication tokens, security keys, encryption keys, passwords / user credentials, etc.)	Will the tools required for the scans/testing be provided by the Bank? What are the tools currently used by the bank for SAST, Penetration Testing, source code review, Configuration review etc?	Bidder has to use their own tools for performing the scans

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
45	70	Annexure-9 Scope of Work	A.2.2	Check for DevSecOps (CI/CD pipeline based Security operations) processes	Please provide the details of your DevSecOps (CI/CD pipeline) environment.	Details will be shared with the selected bidder
46	34	4.Human Resource Requirement	Section G 4	The selected bidder shall provide a contingent of well trained personnel and extend necessary mentoring and operational support to the intermediary network of agents, etc. as part of the solution/service.	We assume that all the activities including the VAPT activities are to be performed onsite from Canara Bank HO. Please confirm	Bidder to comply with the RFP terms and conditions.
47	34	4.Human Resource Requirement	Section G 4	The selected bidder shall provide a contingent of well trained personnel and extend necessary mentoring and operational support to the intermediary network of agents, etc. as part of the solution/service.	Is there any experience criteria for the resources deployed in the project?	Bidder to comply with the RFP terms and conditions.
48	12	9. Scope of Work	9.4	The selected Bidder should have pool of at least twenty (20 Nos) professionals, to deploy on site, in case if required for conducting the assessment, with relevant qualifications and having a minimum of 5 years of experience in conducting the similar kind of assessment.	We assume that the bidder can deploy any number of resources to complete the activities as per the given timelines. Kindly confirm.	Bidder to comply with RFP terms
49	87	Annexure-9 Scope of Work	F.3.1	1. Check the CSP hosting environment SOC2 Type2 report for detailed security controls and their effectiveness status. Enquire with auditee management on controls that are ineffective or qualified by CSP's auditors in the SOC2 Type2 report and assess the compensating controls.	Who is the Cloud Service Provider (CSP)? How many Web/Mobile applications are hosted in Cloud?	The details will be shared with the selected bidder
50	79	Annexure-9 Scope of Work	C	Network Vulnerability Assessment	How many Network devices are in total scope (CBS & Other Critical infra/Apps) for Penetration Testing?	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
51	82	Annexure-9 Scope of Work	E	Network and Device Configuration Review	How many Network and Security devices are in total scope for Configuration review?	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
52	72	Annexure-9 Scope of Work	B	Application Security Assessment (both Black Box and Grey Box)	What is the total count of applications (including web applications and mobile applications) in CBS & Other Critical Infra/Apps for Security Assessment?	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
53	72	Annexure-9 Scope of Work	B	Application Security Assessment (both Black Box and Grey Box)	Do you have any separate test environment/apps to conduct the VAPT Testing?	The details will be shared with the selected bidder
54	72	Annexure-9 Scope of Work	B	Application Security Assessment (both Black Box and Grey Box)	How many rounds of revalidation is in the scope?	The details will be shared with the selected bidder
55	91	Annexure-9 Scope of Work	I	Identity and Access Management (IAM) Controls Review	What is the IAM solution & PAM solution used by Bank?	The details will be shared with the selected bidder
56	89	Annexure-9 Scope of Work	G4	Database Activity Monitoring	Is the Bank using any DAM (Database Access Monitoring) tool for Database Monitoring?	The details will be shared with the selected bidder
57	41	Indemnity	19.6	The limits specified in above clauses shall not apply to claims made by the Bank/third parties in case of infringement of intellectual property rights or loss caused due to breach of confidential obligations or applicable data protection laws or commission of any fraud by the bidder or its employees or agents or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.	Client is requested to delete exceptions to the limitation of liability. The exceptions render the limitation of liability ineffective and make the liability unlimited.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
58	NA	Termination	NA	We do not have any right to terminate	To uphold the principles of natural justice and to bring parity in the contract, we request client to give us the right to terminate the contract in case client breaches any of its material obligations under the contract, provided a notice for such breach is given to client along with a rectification period of 30 days.	Bidder to comply with RFP terms and conditions.
59	NA	Limitation of Liability	NA	Indirect and consequential losses are not excluded from liability	Client is requested to include to clause to state that we will not be liable for any indirect and consequential losses or damages. This is as per GFR and MeitY guidelines and also the industry standard. Even the Contract Act, stipulates and remote and consequential damages are not payable. Client is requested to include the below clause: *"Purchase/Client agrees that Consultant will not be liable for (i) loss or corruption of data from your systems, (ii) loss of profit, goodwill, business opportunity, anticipated savings or benefits or (iii) indirect or consequential loss."*	Bidder to comply with RFP terms and conditions.
60	126	Confidentiality Obligations	12	Obligations to survive is perpetual	We request client to reduce the survival period of confidentiality obligations to one year post expiry or termination.	Bidder to comply with RFP terms and conditions.
61	NA	Confidentiality Obligations	NA	Obligation to return all confidential information / destroy all confidential and no right to retain a copy	We request client to allow us to retain our working papers and a copy of confidential information for our records and any future reference or audit requirements, subject to confidentiality obligations under this Agreement.	Bidder to comply with RFP terms and conditions.
62	36	Publicity	8	Any publicity by the selected bidder in which the name of the Bank is to be used will be done only with the explicit written permission of the Bank	Please appreciate that this is a prestigious project for us and we would like to showcase this project in our future proposals. We request client to allow us to refer to you and the services we have performed for you for citation / reference purposes, as long as we do not disclose your confidential information.	PBidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
63	37	INTELLECTUAL PROPERTY RIGHTS:	9.3	Indemnities for IPR infringement claims without exceptions	We request client to include the following exceptions and procedure as these are industry standards and reasonable. They are also mentioned in the MeitY guidelines. *"1. Notwithstanding anything contained in this agreement, if the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.* *2. Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by: a) Indemnified Party's misuse or modification of the Service; b) Indemnified Party's failure to use corrections or enhancements made available by the Indemnifying Party; c) Indemnified Party's use of the Service in combination with any product or information not owned or developed by Indemnifying Party; However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either: i. Procure the right for Indemnified Party to continue using it; ii. Replace it with a non-infringing equivalent; iii. Modify it to make it non-infringing.* *3. The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement."*	Bidder to comply with RFP terms and conditions.
64	31	Indemnity	12	Indemnity for breach of contract obligations	There are several remedies available under law and contract to you for such breach of obligations. For eg., there are penalties and LDs that may be imposed for some of these breaches. Seeking indemnities for such breaches frustrates the entire purpose of such remedies available to you. We understand that remedies other than indemnity will be sufficient for such breaches. We request you to kindly delete this section. If you still insist on retaining this section, then we request you to make it subject to final determination of court/arbitrator.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
65	NA	Indemnity	NA	Indemnities for tax non payment	In the GST regime, this clause may not be feasible. We request you to kindly delete this clause. Alternatively, kindly limit liability under this clause to reimburse you any penalty / fine that may be imposed on you solely due to breach of GST laws on our part, subject to overall cap of one time the fees payable to us under this agreement.	Bidder to comply with RFP terms and conditions.
66	NA	Indemnity	NA	Indemnities for death and bodily injury	Request client to kindly delete these. Alternatively, kindly cap these indemnities to limitation of liability cap or one time the fees payable to us under this Agreement.	Bidder to comply with RFP terms and conditions.
67	31	Indemnity	12	Indemnities not subject to final determination by court/arbitrator	We agree to indemnify to the extent the damages/losses are finally determined by a competent court or arbitration. Please make indemnities subject to final determination by court/arbitrator. This is also the industry standard and prescribed by MeitY in its guidelines.	Bidder to comply with RFP terms and conditions.
					The indemnities set out in this agreement shall be subject to the following conditions: (i) the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise; (ii) the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense; (iii) if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this clause, the Indemnified Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in losses; (iv) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;	

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
68	31	Indemnity	12	No process for indemnity	(v) all settlements of claims subject to indemnification under this Clause will: a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement; (vi) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings; (vii) the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings; (viii) in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this clause, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and (ix) if a Party makes a claim under the indemnity set out under Clause above in respect of any particular loss or losses, then that Party shall not be entitled to make any further claim in respect of that loss or losses (including any claim for damages).	Bidder to comply with RFP terms and conditions.
69	31	Cancellation	12	Cancellation / Recission of Contract	Cancellation / Rescission means voiding the contract and making the contract ineffective from its inception, thereby restoring the parties to the positions they would have occupied if no contract had ever been formed. In this scenario, bidder may be deprived of any payment and refund of all payments made already may be sought. Request deletion of this clause	Bidder to comply with RFP terms and conditions.
70	15	Penalties/Liquidated Damag	3.2	The total Penalty/LD to be recovered under clause 3.1 shall be restricted to 10% of the total cost of ownership	We request client to cap the liquidated damages/penalties cumulatively to 5% of the total contract value.	Bidder to comply with RFP terms and conditions.
71	NA	Liquidated damages	NA	Not sole and exclusive remedy	We understand that as per Contract Act, where LDs are stipulated, generally any other damages cannot be claimed. Therefore we request you to kindly make imposition of liquidated damages as sole and exclusive remedy for corresponding breaches.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
72	NA	Liquidated damages	NA	Not limited to solely our fault	We understand that we would be liable to pay liquidated damages to the extent corresponding breach is solely attributable to us. Kindly confirm.	Bidder to comply with RFP terms and conditions.
73	NA	IPR	NA	No protection to our pre-existing IPRs	There are innumerable IPRs that exist with us which we would like to use to your benefit while delivering our services to you. These are our pre-existing IPRs and we use it for all clients. We will not be able to give ownership in such IPRs to you just because we are using them for providing services to you, like we use these for other clients. We request that we are allowed to retain ownership of our pre-existing IPRs, else we might be not be able to use these in providing services to you in order to protect our ownership in them. We request you to kindly include the below clause. This is also the standard mentioned by MeitY in its guidelines. *"Notwithstanding anything to the contrary in this agreement, Consultant will retain the ownership of its pre-existing intellectual property rights (including any enhancement or modification thereto) even if such IPRs are used for creating deliverables, are incorporated in the deliverables, etc. To the extent such pre-existing IPRs are included/incorporated in the deliverables, upon receipt of all due and payable payment in full, the Consultant shall grant a non-exclusive, perpetual and fully paid up license to the Purchaser/Client to use such pre-existing IPRs for use of deliverables for the purpose for which such deliverables are meant for client's internal business operations."*	Bidder to comply with RFP terms and conditions.
74	128	Right to Audit	15.3	Widely worded audit rights	We wish to clarify that we will retain our records as per our records retention policies. Upon reasonable notice, we will allow Client to inspect our invoicing records under this engagement; such inspection shall be done in a pre-agreed manner and during normal business hours. For avoidance of doubt, such inspection should not cause us to be in breach of our organizational confidentiality requirements. Please acknowledge that our audit related obligations will be subject to foregoing statement.	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
75	41	Indemnity	19.4.	Obligations to survive for more than a year post expiry or termination of contract	We request that any obligation arising under the agreement shall survive for a period of 12 months, post termination/expiry of the Contract	Bidder to comply with RFP terms and conditions.
76	NA	No third party disclaimer	NA	There is no restriction on the usage of deliverable. No third party disclaimers.	We will be providing services and deliverables to you under the contract. We accept no liability to anyone, other than you, in connection with our services, unless otherwise agreed by us in writing. You agree to reimburse us for any liability (including legal costs) that we incur in connection with any claim by anyone else in relation to the services. Please confirm our understanding is correct.	Bidder to comply with RFP terms and conditions.
77	NA	Acceptance	NA	No acceptance criteria	If the project is to be completed on time, it would require binding both parties with timelines to fulfil their respective part of obligations. We request you that you incorporate a deliverable acceptance procedure, perhaps the one provided by MeitY in their guidelines, or the one suggested below, to ensure that acceptance of deliverables is not denied or delayed and comments, if any, are received by us well in time. You may consider including the below simple clause: *"Within 10 days (or any other agreed period) from Client's receipt of a draft deliverable, Client will notify Consultant if it is accepted. If it is not accepted, Client will let Consultant know the reasonable grounds for such non acceptance, and Consultant will take reasonable remedial measures so that the draft deliverable materially meets the agreed specifications. If Client does not notify Consultant within the agreed time period or if Client uses the draft deliverable, it will be deemed to be accepted."*	Bidder to comply with RFP terms and conditions.

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
78	126	CONFIDENTIALITY AND NON-DISCLOSURE:	12.1	Duty of care is very high - i.e. we need to maintain confidentiality using highest/strictest/best efforts standards;indemnity for Breach	We request client to kindly confirm that we will be obliged to protect Confidential Information using the same degree of care as we use to protect our confidential information of similar nature, and in any event, by using at least reasonable degree of care.	Bidder to comply with RFP terms and conditions.
79	32	Order Cancellation/Termination of Contract	12.3, 12.4	Risk purchase	Request client to limit our liability under this clause to 10% of the value of corresponding goods/services not delivered by us. Please also confirm that client will use government procurement norms (including price discovery) for procurement of such services from third parties.	Bidder to comply with RFP terms and conditions.
80	63	Scope of Work	1.1.Comprehensive audit should cover the entire application, including the following:	(a) Web application (both thick client and thin client);	There is no any cumulative count please provide the same	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
81	63	Scope of Work	1.1.Comprehensive audit should cover the entire application, including the following:	(b) Mobile apps;	1.Total No. (Approximate) of Input Screens 2.Total No. of input fields 3.Number of Web Services, if any 4.Number of methods in all web services 5.Whether audit can be remotely	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
82	63	Scope of Work	1.1.Comprehensive audit should cover the entire application, including the following:	(c)APIs (including API whitelisting);	1.Number of Endpoints hitting by API 2.No. of API(s) per Endpoint 3.No. of Methods/Function calls per API 4."Average number of input or parameters per Method/Function call per API"	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
83	63	Scope of Work	1.2. The scope of the comprehensive audit Should include, inter alia, the following:	(a) Source code assessment	1.Total No. (Approximate) of Input Forms 2. No. of Lines of Code	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
84	63	Scope of Work	1.2. The scope of the comprehensive audit Should include, inter alia, the following:	a) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IR AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs);	Please provide counts:- 1.Total No. of Nodes 2.No. of Servers with details (Windows, Linux, Sun Solaris etc) 3.No. of Desktops/Laptops 4.No. of Routers 5.No. of Switches (L3, L2 with details) 6.No. and make of firewalls/ UTM devices 7.No. of IDS/IPS 8.No. of Wireless Access points	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
85	12	9	Scope of Work	-	Kindly confirm if client is looking for a checklist audit against the controls mentioned in the RFP or SISA should help in compliance	The bidder has to conduct the audit as per the Scope of Work
86	14	Section C	Scope of Work	1.4	No. of Web Applications in Scope for App PT activity *Small Size App(Less than 40 menus) **Medium Size App(Between 40 - 80 menus) ***Large Size App(Above 80 menus)	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
87	14	Section C	Scope of Work	1.4	No. of Mobile Applications in Scope (Android + IOS) for App PT activity *Small Size App(Less than 40 menus) **Medium Size App(Between 40 - 80 menus) ***Large Size App(Above 80 menus)	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
88	63	Annexure 9	Scope of Work	1	No. of Internal IPs in scope for Internal VAPT activity	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
89	63	Annexure 9	Scope of Work	1	No. of External IPs in scope for External VAPT activity	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
90	63	Annexure 9	Scope of Work	1	No. of API Calls for API Security Testing (please share the count of API calls for Each API domain/Service (Excluding internal API calls made by apps in scope above)	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
91	63	Annexure 9	Scope of Work	1	Please highlight the requirement for Secure Code review activity. If yes, please confirm on the total count of Web apps along with total count of count of LOCs for each applications separately. *Small Size app(Less than 100K LOCs) **Medium Size app(Between 100K - 200K LOCs) ***Large Size app(Above 200K LOCs)	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
92	64	Annexure 9	Scope of Work	1	No. of Assets for Configuration Review No. of Network Devices No. of Servers	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
					Please specify the objective of the Audit?	As per the Scope of Work of RFP
					Please highlight the count of Applications in scope and also brief about the applications	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
					Please highlight the count of Network Devices in scope	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
					Please highlight the count of Servers in scope	Bidders to refer Corrigendum-1. The indicative count is available in Annexure-14 Bill of Material
					Please highlight the number of departments in scope	The details will be shared with selected bidder
					Please highlight the number of people in scope	The details will be shared with selected bidder

Sl. No.	Page no.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
93	63	Annexure 9	Scope of Work	1	Please Highlight the count of locations in scope(**Ex: Corporate Office, Data Centers, DR Sites etc).**	Bangalore and Mumbai
					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.	The details will be shared with selected bidder
					Please highlight the delivery mode of the project (remote or onsite).	Onsite
					Please specify, whether policy & procedure support* is required (*Sharing the templates and assisting the customer in filling up of the policy & procedure)	Bidder has to conduct audit as per the Scope of Work mentioned in the RFP
					Please mention the start date of the Project?	The details will be shared with selected bidder
					Please mention the expected end date of the project(Deadline)?	The details will be shared with selected bidder
					Please confirm, how many Sub entities that has to undergo AUA/KUA audit?	NIL

Date: 21/06/2024
Place: Bengaluru

Deputy General Manager