CENTRAL BANK OF INDIA, Tender No-CO:CA&ID:PUR:2022-23: 01 'Cyber Security Audit and Comprehensive Audit of CBS Project & other applications' 2021-22 & 2022-23.

CORRIGENDUM No. 02

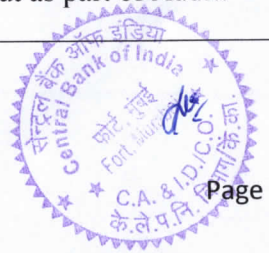
S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
1	1	Application Audit	*Complete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) including EOD Process of CBS and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), UPI, RTGS/ NEFT / SWIFT, ATM Transactions, Financial Inclusion (FIGS/ADV), Integrated Treasury, Dealing Room operations, In-house developed applications etc. (59 applications apporx).*	Request you to provide a count of application in terms of no of pages a. API/ Web services b. Small (1-50 pages) c. Medium (50-100 pages) d. Large (100-250 pages) e. V Large (more than 250 pages)	Count of application in terms of no of pages a. Small (1-50 pages): 21 b. Medium (50-100 pages): 13 c. Large (100-250 pages): 13 d. V Large (more than 250 pages): 12
2	1	Application Audit	Complete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) including EOD Process of CBS and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), UPI, RTGS/ NEFT / SWIFT, ATM Transactions, Financial Inclusion (FIGS/ADV), Integrated Treasury, Dealing Room operations, In-house developed applications etc. (59 applications	*Request you to confirm if Black-box (PT) or Grey-box testing (Application security)or White box testing (Application Secure Code review) or all of these are to be performed on these applications*	Application Security audit to be carried out

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			apporx).		
3	1. 2	2. DC, DRC & Near Site Audit	Thorough Audit of bank"s Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad and Near Site at Navi Mumbai.	*Request you to confirm if the audit has to be carried out remotely or on-site*	Audit is to be carried out onsite only
4	1. 2	2. DC, DRC & Near Site Audit	Audit of Disaster Recovery and Business Continuity Plans for adequacy and conformance of BCP guidelines.	*Request you to confirm that the audit shall be carried out basis the RBI BCP guidelines only*	Audit is to be carried out in line with RBI BCP Policy, ISO: 27001: 2019 and Bank's Business Continuity Management Policy.
5	1.3	3. Network / Cyber Security Audit	Audit of effectiveness of Anti-virus system.	*Request you to elaborate on the scope of this activity*	To audit the effectiveness of Bank's existing Antivirus solution as per RBI and Bank's policies.
6	1. 3	Configuration Audit:	Configuration audit of various devices, especially for network & network security devices	*Request you to kindly confirm the segregated out of devices for which configuration review of to be performed* *a. Router* *b. Switches* *c. Firewall* *d. Other network device*	Configuration audit of network devices and network security devices are to be carried out.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
7	1.4	Audit of ATM project	Security audit of ATM switch, ATM card related operations.	*Request you to confirm on the count of ATM switch in scope for audit*	Both ATM switch and ATM card related operations are in the scope of Audit.
8	1.5	Outsourcing Audit	Covering audit of Information System, functional and operational aspects of Outsourced activities as per Guidelines of RBI. Outsourced activities/ vendor of DIT, ATM Dept., Call Centre, Financial Inclusion, Debit Card and other outsourced activities. (Approximate 68 outsourced activities)	*request you to confirm our understanding that sample outsourced activities shall be taken in scope for audit*	Comprehensive outsourcing Audit is to be carried out.
9	6	Bid Cost	non-refundable bid cost of Rs. 10,000/- by demand draft/ banker's cheque in favour of Central Bank Of India.	*As we are a MSME enterprise. Please confirm if it is mandatory for us to provide Bid - Cost. Please clarify if we can be exempted from this clause.*	Government directives will be considered provided the bidder is genuine Micro & small Enterprises and proves the eligibility.
10	15	EMD	Bidder should also submit refundable EMD - Earnest Money/Bid Security deposit of Rs. 50,000/-.	*As we are a MSME enterprise. Please confirm if it is mandatory for us to provide EMD Please clarify if we can be exempted from this clause.*	Government directives will be considered provided the bidder is genuine Micro & small Enterprises and proves the eligibility.
11	19	Eligibility Criteria	The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum one each from :- a).	*We are a cyber security consulting firm and we have multiple experienced consultants. As ACA/FCA certifications are focused on financial*	All requirements under Eligibility Criteria are mandatory. However availability of CA will suffice the requirement of ACA/FCA

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH	*aspects which is not useful for Central Bank of India' s requirements. Please let us know if ACA/FCA certifications is mandatory for clearing the eligibility criteria. Please note, we do have a certified chatered accountant (CA) working in our firm.*	certifications.
12	19	Eligibility Criteria	The Bidder (i) should be in existence for at least five years as on 31.03.2022	*Audit firm was established on July 2017 and we are a MSME Enterprise. We completed five years on 07.07.2022.*	Please refer Addendum/ Corrigendum No. 01 uploaded on 20.08.2022
13	32	On-Site	Location of audit will be DC at Navi Mumbai, Near Site at Navi Mumbai, DRC at Hyderabad, and various departments of Central Office at Mumbai. Site/ locations of Outsourced vendors will be provided separately to selected bidder.	*Due to the ongoing pandemic situation, can we conduct all the activities remotely and there will be no On-Site appearance of any Audit Firm's Employees. At present we have conducted multiple audits similar to your requirements for multiple banks of all categories remotely.Please clarify if we can be exempted from this clause.*	Audit to be carried at Onsite only
14	33	Performance Bank Guarantee (PBG)	The successful bidder will have to give Performance Bank Guarantee for 3% of the total project cost, while submitting the acceptance of	*As we are a service provider and an MSME enterprise. Please confirm if it is mandatory for us to provide PBG. Please clarify if we can be exempted*	Government directives will be followed in this regard.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			order. The validity of the Performance Bank Guarantee should be for 8 months, if required, it should be renewed till completion of the audit.	*from this clause.*	
15	34	Penalty	Delayed start of audit, delayed completion of audit and delayed submission of report as per agreed terms defined in the RFP will attract penalty of 0.5% per week on delay of total amount payable for audit assignment (maximum up to 15% of the fees), if the delay was solely the auditor's fault and reasons not attributable to Bank.	*We provide cyber security consulting services and implementation of all the services will have a dependency on both CyRAACS as well as the client (in this case - Central Bank of India), So the possibilities of delay in completion of project will fall on both the parties. Please let us know if this clause can be removed.*	Penalty clause is clearly spelt, hence no change is required.
16	5	Configuration Audit	Configuration audit of various devices, especially for network & network security devices.	*1. Do we have to conduct configuration check for all the network and security devices or sampling methodology to be considered?* *2. If sampling to be considered what is the sampling size?*	1. Sampling is to be done for each type of Network devices. 2. Sampling size for Network devices will be approximately 20. However Vulnerability assessment of all Servers, Network Devices and Security Devices are to be carried out as part of Audit.



S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
17	32	Vendor Audit and ATM Audit	Location of audit will be DC at Navi Mumbai, Near Site at Navi Mumbai, DRC at Hyderabad, and various departments of Central Office at Mumbai. Site/ locations of Outsourced vendors will be provided separately to selected bidder.	*1. Do we have to conduct Vendor Audit on site or remotely?* *2. Do the bank has a Vendor Check List to be followed?*	1. Vendor Audit to be carried out Onsite. 2. Annexure-D of the RFP documents is to be referred for the Vendor list. Audit to be carried out as per RBI's and Bank's Outsourcing policy and scope of the RFP docuement.
18	32	Vendor Audit	Selected vendor has to submit location-wise reports i.e. separate reports for technical and functional observations.	*1. Please confirm, Should CyRAACS support on the submission of some report as an External Audit?* *2. Do we have to sumbit a separate report for the following:-* *CSF, DPSC, UIDAI, UPI, NPA*	The scope of Audit reports is clearly mentioned in the RFP document.
19	6	Invitation for Tender Offers	A complete set of tender documents may be purchased by eligible bidder upon payment of a non-refundable fee of Rs.10,000/-(Rupees Ten thousand only) by demand draft/ banker's cheque in favour of Central Bank Of India, payable at Mumbai or through online payment, details of which is given below.	*We are registered with NSIC and MSME. As per the Government guidelines, NSIC and MSME registered companies are expemted from paying the amount of EMD for any Tender issued in India.* *Considering the same, kindly exempt us from the submission of EMD and Tender Fees*	Government directives will be considered provided the bidder is genuine Micro & small Enterprises and proves the eligibility.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
20	15	ENVELOPE-III (EMD AMOUNT)	Bidders are required to give a Demand Draft drawn in favor of Central Bank Of India, payable at Mumbai, (valid for 90 days from the due date of the tender) for Rs.50000/-(Rupees Fifty Thousand only) as Earnest money Deposit (EMD) (non-interest bearing) along with their offer. Aalternatively the bidder may pay the Earnest Money Deposit online as per details furnished here below:	*We are registered with NSIC and MSME. As per the Government guidelines, NSIC and MSME registered companies are expemted from paying the amount of EMD for any Tender issued in India.* *Considering the same, kindly exempt us from the submission of EMD and Tender Fees*	Government directives will be considered provided the bidder is genuine Micro & small Enterprises and proves the eligibility.
21	51		Application Security and Controls for CBS and Other applications	*1. Please confirm how many applications are in scope of this engagement apart from CBS.* *2. Please provide details of each application along with no. of dynamic pages and no. of user roles.*	1. Annexure-C of the RFP document is to be referred for list of applications. 2. Count of application in terms of no of pages a. Small (1-50 pages): 21 b. Medium (50-100 pages): 13 c. Large (100-250 pages): 13 d. V Large (more than 250 pages): 12
22	52		Review of operating system and Data Base Controls	*1. Please confirm how many OS, servers, DB need to be reviewed from secure configuration perspective.*	Total number of Physical/Virtual Servers (OS instances) at DC and DRC is around 1400. Number of DB instances is around: 100.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
					Number of Network devices at DC and DRC is around: 225.
23	54		*Vulnerability assessment of all the critical servers/ devices (1.2 & 2.5)*	1. Please provide number of critical server/devices for vulnerability assessment. 2. Would this be authenticated scan or unauthenticated?	1. All Servers and Devices at DC, DRC and Near Site (Near DC) are part of vulnerability assessment. 2. This is to be authenticated scan.
24	57		*NETWORK INFRASTRUCTURE AND CYBER SECURITY AUDIT - Network VA & Config Review*	1. Confirm no. of external and internal IPs for network VA 2. Would this be authenticated scan or unauthenticated? (Network VA) 2. Confirm no. of network devices for Config Review - Routers , Switches, Firewalls, Security Devices etc.	1. Around 1400 number of Servers and 225 number of Network devices at DC, DRC and Near Site ar part of network VA. 2. There should be authenticated scan 3. Total 225 number of network devices including Routers , Switches, Firewalls, Security Devices etc are part of Config Review.
25	59		*NETWORK INFRASTRUCTURE AND CYBER SECURITY AUDIT - Penetration Testing*	Are these applications different than applications covered in "Application Security and Controls for CBS and Other applications"? 2. If not, please provide details of each application along with no. of dynamic pages, no. of user roles and supported OS (Android and iOS).	List of applications is mentioned in Annexure-C of the RFP document.
26	66		*SCOPE FOR AUDIT OF OUTSOURCING ACTIVITIES -*	1. Confirm no. systems/Applications to be reviewed along with no. of pages	Approximate number of Servers and Network devices under the

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			VAPT Audit of FIGS & ADV	& roles	Audit scope are 1400 and 225 respectively. Count of application in terms of no of pages a. Small (1-50 pages): 21 b. Medium (50-100 pages): 13 c. Large (100-250 pages): 13 d. V Large (more than 250 pages): 12
27	5		*1. Application Audit: Complete review of applications and security audit of all major applications including Core Banking Application (CBS-B@ncs24) including EOD Process of CBS and Delivery Channels i.e. Internet Banking, Mobile Banking (SMS/ WAP), UPI, RTGS/ NEFT / SWIFT, ATM Transactions, Financial Inclusion (FIGS/ADV), Integrated Treasury, Dealing Room operations, In-house developed applications etc. (59 applications approx.).*	1. We would be doing only technical review. Please confirm. 2. Kindly confirm the number of vendors involved. Please clarify if onsite vendor audits needs to be performed.	1. The scope is clearly mentioned in the RFP document. 2. Annexure-D of the RFP document is to be referred for the list of Vendors.
28	5		*Audit of effectiveness of Anti-virus system*	Kindly elaborate on the expectations from the bidder.	To audit the effectiveness of Bank's existing Antivirus solution as per RBI and Bank's policies.
29	5		*Outsourcing Audit:- Covering audit of Information System, functional and operational aspects of Outsourced activities as per Guidelines of RBI. Outsourced*	Kindly confirm if the onsite audit needs to be performed for the vendors.	Onsite audit needs to be performed for the vendors.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			activities/ vendor of DIT, ATM Dept., Call Centre, Financial Inclusion, Debit Card and other outsourced activities. (Approximate 68 outsourced activities)		
30	6		*Comprehensive System audit of Core Banking Solution (Finacle) of 2 RRBs (UBGB & UBKGB) sponsored by Central Bank of India and having their Data Center at Navi Mumbai, Maharashtra*	Kindly confirm the CBS systems in use for all three banks in scope, please provide the details.	CBS systems in use for Bank is B@ncs-24 and for two RRBs is Finacle.
31	30		*Scope Of Work- The IS Audit should comply the various guidelines issued by RBI time to time.*	Kindly provide the list of all the guidelines to be considered for the reviews	Under the scope of Bidder.
32	31		*Purpose of the Comprehensive audit - Application meets the industry best practices securities standards*	Kindly provide the list of standards to be referred.	Under the scope of Bidder.
33	41		*Annexure 3: Commercial Bid - Rate per Man Months (b)*	Kindly provide the rate per man months to be considered.	Bidder is required to quote.
34	41		*Annexure 3: Commercial Bid - COMMERCIAL FOR 2nd YEAR (Y=X)*	Kindly confirm if the bidder is expected to perform the review for two years (i.e. for two cycles)	Yes, the bidder is expected to perform the review for two years (i.e. for two cycles)
35	42		*Annexure 4: Format of curriculum vitae (CV)*	Kindly confirm the no of resources CVs to be shared.	CVs of minimum 06 permanent experts/ certified resources to be shared with minimum one each from each field explained at Sr. no. 4 of "Format for Technical Bid at page no. 18.
36	45		*To ensure appropriate testing of various controls including input,*	Kindly elaborate on the expectations from the bidder. We would be	As part of the scope, Bidder is required to carry out Testing/ Audit

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			process and output controls which would result in : • *Greater Comfort &* • *Enable the banks management to place reliance on the new solution/ initiatives being deployed*	providing recommendations only.	and provide comprehensive report along with recommendations and mitigation methodology.
37	45		*Audit of Data Centre & Disaster Recovery, Network infrastructure & cyber security and its compliance with industry best security standards & practices .*	Kindly confirm if any recognized standards needs to be referred	Industry standards to be referred.
38	47		*The Scope of work is broadly as under - Major Aspects to be covered*	We will be performing only technical review and no functional review. Please note KPMG does not provide any legal services and we does not conduct financial audit.	The complete scope of the RFP document is to be adhered.
39	51		*Study & review the implemented functionality of Core Banking Solution (B@ncs24) & allied modules/ applications in all the areas and to ensure correctness of functionality of each module & all modules in totality including parameterization with reference to the specifications given in the CBS RFP & other applications RFP floated and the procedure of the bank for all the modules like Retail deposits, advances, Trade Finance, Bills, Lockers, MIS etc.*	We will be performing only technical review and no functional review. Please confirm	The complete scope of the RFP document is to be adhered.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
40	51		*Review of the application security features built within CBS and other application (list mentioned below) and also the Security and controls built in and around the operating system and data base used by the Core Banking Application (B@ncs24) both at the central level and at the client level. ISO 27001 guidelines, Web application security and other security related guidelines are to be observed.*	Kindly confirm if any recognized standards/ guidelines needs to be referred	Industry standards to be referred.
41	52		*System development – Problem / opportunity definition, Management of Change process, analysis of existing system, formulation of requirement, application Software development, procedure development, acceptance testing.*	Kindly confirm the count of SDLC developed In house or by Vendor	There is an average of 15-20 nos of SDLCs per month both developed In house and by Vendor.
42	53		*Change Management control - Standard instruction charge (Global)*	Kindly specify if any regulatory guidelines needs to be referred.	Industry standards to be followed.
43	54		*Reconciliation of foreign exchange positions between the dealers' records and the accounting system.*	We would be conducting only process review and functional testing is not part of the scope.	No change in RFP clause.
44	54		*changes in the EDP systems*	This is not included n the list of application mentioned below, kindly clarify if the application is part of the scope	This is part of Infrasctructure and applications mentioned in the RFP document.
45	60		*Network Architecture review should be carried out for security and*	We would only check for completeness and accuracy of data	The complete scope of the RFP document is to be adhered.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			performance which include the following:	elements. Please confirm	
46	61		*Capacity Planning*	Please confirm the no of servers and devices to be considered as part of scope	Approximate number of Servers and Network devices under the Audit scope are 1400 and 225 respectively.
47	61		*Performance Audit - Link Level*	Please confirm if scalability needs to be checked	Scalability of Links are part of Audit.
48	64		*SCOPE FOR AUDIT OF ATM PROJECT - Review of Operations at Switch*	1. Kindly confirm the count of vendors involved. Please confirm if onsite audit needs to be conducted. 2. Please confirm if the audit needs to be performed against the RFP issued also.	1. Annexure-D of RFP document is to be referred. 2. Audit needs to be performed against the Purchase Orders issued to Vendors.
49	67		*SCOPE FOR AUDIT OF OUTSOURCING ACTIVITIES - Procedural & Operational aspects*	1. We understand only policy review is part of the scope and creation of policies is not included as part of the scope. 2. Please confirm if onsite vendor audit needs to be conducted. If yes, kindly provide the list of the vendors.	1. Creation of policies is not included as part of the scope. 2. Annexure-D of RFP document is to be referred.
50	98		*Annexure- 7: Scope of IS Audit of RRBs*	Please confirm if onsite audit of RRBs is required	Onsite audit of RRBs is required.
51	98		*Audit of bank's Data Centre (DC) at Navi Mumbai, Disaster Recovery Centre (DRC) at Hyderabad*	We understand the DC is same for CBI and RRBs, please clarify and confirm	DC and DRC of Bank and RRB are co-located in respective Cities.
52	98		*Audit of Delivery Channels – Internet Banking, Mobile Banking (SMS/WAP), NEFT, FI, AEPS, BHIM-Aadhaar, IMPS etc.*	We understand the delivery channels are same for CBI and RRBs, please clarify and confirm	Delivery Channes of RRBs are limited to RTGS, NEFT, ATM, FI, IMPS, Internet Banking,

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
53	99		*Application Review Scope - Functionality implemented vis-à-vis the Bank's requirements*	Kindly elaborate on the expectations from the bidder.	To audit whether the functionalities imnplemented in the Application ar in line with the Bank's requirements.
54	100		*Application review of the software for Core banking solution i.e. Finacle - Identify key functionalities not supported by the application*	Kindly elaborate on the expectations from the bidder, also please confirm if we have to follow any standard or guidelines	Key functionalities in line with Business requirements and Policies of Bank and policies of Govt. of India, Statutory requirements.
55	34		*Delayed start of audit, delayed completion of audit and delayed submission of report as per agreed terms defined in the RFP will attract penalty of 0.5% per week on delay of total amount payable for audit assignment (maximum up to 15% of the fees), if the delay was solely the auditor's fault and reasons not attributable to Bank.*	Request to modify the clause as : "Delayed start of audit, delayed completion of audit and delayed submission of report as per agreed terms defined in the RFP will attract penalty of 0.5% per week on delay of total amount payable for audit assignment (maximum up to 10% of the fees), if the delay was solely the auditor's fault and reasons not attributable to Bank)"	No change in RFP terms.
56	125		*Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all copies, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with*	Request to modify the clause as : "Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information, abstract, extracts, samples, notes or modules thereof to the Disclosing Party within seven (7) days after receipt of notice, and (iii) upon request of the Disclosing Party, certify in writing that the Receiving Party has complied with the	No change in RFP terms.

S No	Section No/ RFP Page No.	Section Name/ RFP Clause	RFP Statement/ Clause	Query	Bank's Response
			the obligations set forth in this paragraph.	obligations set forth in this paragraph."	
57	NA		*General*	In accordance with standard industry practice, our aggregate liability under this RFP and in connection with the services shall be for direct damages and shall, in all circumstances and events, be limited to one time the fees paid to us. We shall not be liable for any indirect or consequential losses	No change in RFP terms.
58	NA		*General*	1. confirm if all Security Testing activities will be conducted from Bank's premises.	Other than Penetration Testing of Internet Facing applications, all Security Testings/Audits to be carried out from Bank's premises.