Corrigendum 01: RFP for 'Cyber Security audit and Comprehensive Audit of CBS Project & other applications'– 2024-25 & 2025-26

Sl No.	Clarification Point	Query	Bank's response
1	Tender Document Cost & Earnest Money Deposit	Could we get an exemption from the EMD and Tender Fee as we are MSME Certified.	Yes
2	The Bidder must have a minimum turnover of INR 10 crore (Ten Crore only) per annum out of its IT / Audit / Security operations for the past 3 years.	As we are MSME certified, Shall we get any wavier in this turnover critieria	No change
3	The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH	Is it mandatory to submit every certificate in this requirement?	Self declaration
4	The Bidder should be in existence for at least five years as on 31.03.2024 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and should have done audits as above in 2 Banks out of which at least one in a Public Sector bank in India. Certificate from the bank to that effect to be submitted.	As per our understanding, you require Audit Work Completion Certificate only. Please confirm.	Yes, Certificate is mandatory
5	Period	Please confirm the complete duration for completing the activity is 10 weeks or 7 months.	Total project period is 29 weeks which is equal to approximately 7 months

6	VAPT (Vulnerability Assessment & Penetration Testing) : VA (Vulnerability Assessment) of all major applications including CBS & Delivery Channels, and Penetration Testing of public facing applications viz. Internet Banking, Mobile Banking, Corporate Website, Financial inclusion (FIGS & ADV) etc. VAPT is to be conducted only once in 2024-25 and twice in 2025-26.	As per given pointer, we have to conduct VAPT for FY 24-25 Once in this year and Twice in FY 25-26 but the contract duration is only for one year. Please confirm our understanding or else clarify. AND Kindly provide No.of Application for VAPT (Web & Mobile and No.of Network Devices).	Contract is for 2 FY, i.e. 2024-25 and 2025-26. VAPT is to be conducted only once in 2024-25 and twice in 2025-26. In 2024-25, VAPT is included in IS Audit. In 2025-26, one VAPT is included in IS Audit. Second VAPT is done again after the completion of IS Audit in the same FY.
7	Cloud security Audit of application hosted in public cloud.	No. of Subscriptions? No. of EC2 Instances (VMs)? No. of VPC- Vnets? No. of Load Balancers? No. of VPN Gateways? No. of Storage Accounts?	No. of Subscriptions =5 No. of EC2 Instances (VMs) = 20 No. of VPC- Vnets = 16 No. of Load Balancers = 10 No. of VPN Gateways = 14 No. of Storage Accounts = Nil
8	3.3 Network Architecture Audit:	No.of Network Diagram	There is only one network diagram of the Bank which is to be reviewed

9	Audit of Security Operation Centre (SOC)	Kindly provide below details for the SOC audit Database Server Web Server Mail Server FTP Server Proxy Server DNS Server Application Server RAS Server Other Server IDS / IPS Switch Router Firewall Virtualization Server Other Applications Other Devices Do you conduct Vulnerability Assessment / Penetration Testing? Do you conduct Application Security Assessment? Are you currently using any syslog / any log management solution? Is Network Monitoring System deployed? Have you evaluated any SIEM tool earlier? Brief on the requirement and expectation from SOC / SIEM?	The details will be shared only with successful L1 bidder
10		1. Number of Resources required. 2. Resource qualification. 3. Is everything On-site?	1. To be decided by the Bidder 2. As per qualification mentioned under Eligibility Criteria in the RFP 3. Yes
11	Number of applications and Vendors	Application Audit: if functionality Audit expected here? Please provide more clarification/details on applications and vendors w.r.t Audit.	No Number of application is 100 to 120. Number of vendors is 90 to 110. Details of application and Vendors will be provided to L1 bidder

12	Scope of work	Please confirm which checklist is to be followed for the audit of UBGB or UBKGB.	Scope of work is alredy defined in the RFP
13	Number of ACA/ FCA on the permanent roll of the organization.	We request the client to modify this clause to identify number of CISA / CISM professionals which is more relevant for this project.	No change
14	Technical Evaluation	We request the Bank to publish the technical scoring criteria for each parameter.	scoring criteria is mentioned on Page 29 for Technical evaluation
15	Technical Evaluation criteria #7 Number of completed audit which includes Cyber Security, Network Audit, DC/DRC audit and CBS & other application software audit in Private Sector Bank/ PSU Banks (Excluding Co-operative banks) in last three years	We request the bank to change this criteria to last 5 years. We request the Bank to consider ongoing projects as well.	No change
16		What is the core Banking product used by the Bank?	Bancs@24
17	Scope of work	Application audit: Critical OWASP vulnerabilities: How many applications to be covered in application audit ? Is black box testing expected or grey box testing is expected? Kindly share the average number of dynamic pages per application.	No. of applications will be 100-120. Black box testing needs to be done for 45 applications. Grey box testing for all applications
18	Scope of work	Application audit: VAPT: Please confirm the number of OS, servers, desktops, network devices and appliances to be covered in VAPT. The numbers should be provided for each cycle of audit	There are 2000 Servers VMs in each cycle
19	Scope of work	Configuration audit: Is this to be done on sample basis? If no, kindly share the number of devices for which the configuration review is to be done.	This can be done on sample basis.
20	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 share the number of modules for each RRB.	30-35
21	Vulnerability / Threat / Risk (VTR) Assessment of Bank's Critical Information Infrastructure (and their associated dependencies) as per NCIIPC guidelines	Kindly provide a detailed scope	3 Applications and its associated dependency. It may vary as per Govt of India guidelines.
22	API Security Review.	How many APIs to be covered in this activity?	1000 approximately
23	Secure Configuration Review of Servers and Network Devices.	How many devices to be covered for this activity?	350 Network devices approximately

24	Various applications under CentNeo platform as & when it goes Live during the Audit period	Please explain this requirement in detail.	At present Cent Neo is having 9 application which includes Live or yet to be Live applications. The count is already considered in application count which is 100-120.
25	Cloud security Audit of application hosted in public cloud.	Which public cloud is being used by CBI?	AWS
26	Application Bug finding through automated tool.	Please explain this requirement in detail. Is the requirement to identify functional bugs? Functional bugs should be ideally reported by user teams.	Auditor is expected to find bugs in the applications through some Automated tool(s).
27	Apsec audit of Mobile applications	How many mobile applications are in scope? Kindly share avg number of dynamic pages.	15
28	DAST and SAST of container images	Is this a one time activity? If yes, how many container images are in scope?	No. 17 cluster and 260 nodes
29	Audit of NoSQL and RDBMS Databases.	How many database are in scope?	Will be shared with successful bidder.
30	Audit of VMWare, Nutanix, Microsoft Hypervisor, Openshift Container platform.	Kindly provide a detailed scope	configuration audit of Hypervisor, Container
31	Process Audit of DevSecOps / CICD Pipeline	Please share details about the existing pipeline? Which products are used? How many applications are integrated?	GitLab and Jenkins
32	NA	Does the Bank have any tool for performance audit?	Will be shared with successful bidder.
33	NA	We request the Bank to kindly provide additional 7 working days to submit the proposal. This is in lieu of the financial year end activities.	There is no change in timeline to submit the Bid as on date but if there is any change in timeline then it will be informed on or before 21/03/2024 on Bank's website.

34	**4.15, Short Description of Eligibility Criteria** **Sr. No. 2)** Vendor should have the experience of conducting audit from any three of the following core areas: 1.CBS Application Functionality audit and post implementation 2.Audit of DC/DRC/ Near site 3.Networking audit 4. Cyber Security audit 5.IS Audit/System audit of Delivery channel for Two Banks out of which at least one should be Public Sector Bank in India.	Request you to modify the clause as below: Vendor should have the experience of conducting audit from any three of the following core areas: 1.CBS Application Functionality audit and post implementation 2. Audit of DC/DRC/ Near site 3. Networking audit 4. Cyber Security audit 5. Application Security Audit 6. VAPT 7. Red Team Assessment 8. Digital Forensic Readiness 9. RBI Compliace Assessment 10. Pre-Live Audit 11. IS Audit/System audit of Delivery channel for two PSU/ Scheduled Commercial Banks/ BFSI/ FI in India.	No change
35	**4.15, Short Description of Eligibility Criteria** **Sr. No. 4)** The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH	Request you to modify the clause as below: The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP/ OSCP/ CRTP f). CEH	No change
36	**4.15, Short Description of Eligibility Criteria** **Sr. No. 8)** The Bidder (i) should be in existence for at least five years as on 31.03.2024 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and (ii) Should have done audits as above in 2 Banks out of which at least one should be a Public Sector bank in India. Certificate from the bank to that effect	Request you to modify the clause as below: The Bidder (i) should be in existence for at least five years as on 31.03.2024 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and (ii) Should have done audits as	No change

	to be submitted	above in two PSU/ Scheduled Commercial Banks/ BFSI/ FI in India. Certificate from the bank to that effect to be submitted.	
37	**4.15, Support Document to be submitted** **Sr. No. 10)** Necessary Certificates having executed orders of aggregate value of minimum Rs. 50 lacs during last three financial years for Information Systems Audit including that of Cyber Security / CBS Application /Functionality Audit/ Audit of DC / DRC, Networking Audit, IS Audit / System Audit of CBS / Delivery channel Audits (This certification is in addition to the copies of purchase orders enclosed)	Request you to modify the clause as below: Necessary Certificates having executed orders of aggregate value of minimum Rs. 50 lacs during last three financial years for Information Systems Audit including that of Cyber Security / CBS Application /Functionality Audit/ Audit of DC / DRC, Networking Audit, IS Audit/ Red Team Assessment/ VAPT/ Application Security Assessment/ Digital Forensic Readiness/ System Audit of CBS/ RBI Compliance Assessment/Pre-Live Audit/ Delivery channel Audits (This certification is in addition to the copies of purchase orders enclosed)	No change
38	**4.15, Additional information for Technical Bid Evaluation Criteria (Particulars):** **Sr. No. 7)** Number of completed audit which includes Cyber Security, Network Audit, DC/DRC audit and CBS & other application software audit in Private Sector Bank/ PSU Banks (Excluding Co-operative banks) in last three years.	Request you to modify the clause as below: Number of completed audit which includes Cyber Security, Network Audit, RBI Compliance Assessment, Red Team Assessment, VAPT, IS Audi, Pre-Live Audit, Digital Forensic Assessment, DC/DRC audit and CBS & other application software security audit in PSUs/ BFSI/ FI/ Scheduled Commercial Bank in India in last three years.	No change

39	**5. Qualification Criteria** 5.1.2 The bidder should be a reputed IT Auditing company / Firm having existence in India and should have the experience of conducting Audit from any three of the following core areas : -CBS Application functionality audit and Post Implementation review Audit -Networking Audit -Cyber Security -DC/ DRC Audit -IS Audit / System Audit of Delivery Channels -VAPT of at least One Public Sector Bank in India.	Request you to modify the clause as below: 5.1.2 The bidder should be a reputed IT Auditing company / Firm having existence in India and should have the experience of conducting Audit from any three of the following core areas : -CBS Application functionality audit and Post Implementation review Audit -Networking Audit -Cyber Security -DC/ DRC Audit -IS Audit / System Audit of Delivery Channels -Application Security Audit -Digital Forensic Readiness -Red Team Assessment -Pre-Live Audit -VAPT of at BFSI/ FI/ PSUs/ Scheduled Commercial Bank in India.	No change
40	**5. Qualification Criteria** 5.1.4 The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum, one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP f). CEH	Request you to modify the clause as below: 5.1.4 The bidder's Audit team shall consist of minimum 6 permanent experts/ Certified resource with minimum, one each from :- a). ACA/FCA b). CISA c). CISSP/ CISM d). ISO 27001 LA/ ISO 22301 LA e). CCNP/ CCSP/ OSCP/ CRTP f). CEH	No change
41	**5. Qualification Criteria** 5.1.8 The Bidder should be in existence for at least five years as on 31.03.2024 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and should have done audits as above in 2 Banks out of which at least one in a Public Sector bank in India. Certificate from the bank to that effect to be submitted.	Request you to modify the clause as below: 5.1.8 The Bidder should be in existence for at least five years as on 31.03.2024 (In case of mergers/ acquisitions/ restructuring or name change, the date of establishment of earlier/ original Partnership Firm/ Limited Company can be taken into account) and should	No change

		have done audits as above in 2 BFSI/ FI/ PSUs/ Scheduled Commercial Bank in India. Experience in bank will be preferred.	
42	**5.2) Technical Bid Evaluation Criterai**	Technical bid evaluation does not include below mentioned criteria: 1. Financial capabilities of vendors 2. Additional marks for presentation which will showcase the scope/project understanding of the bidder	1. refer point 5.1.1 2. No change
43	Page no. 5	No. of roles in case of Greybox testing	Will be discussed with the successful bidder.
44	Page no. 5	Count of application for Blackbox testing, if any	Will be discussed with the successful bidder.
45	Page no. 5	Configuration Audit - No. of devices to be considered for the configuration audit.	There are 350 no of Network devices approximately.
46	Page no.6, Point no. 10 & 11	Is It about Secure Configuration Review of Various applications under CentNeo platform as & when it goes Live during the Audit period ? And Secure Configuration Review of Integrated Call Centre ? If yes, what will be the number of application in scope and what would be the frequency of Secure Configuration Review per annum ?	At present Cent Neo is having 9 application which includes Live or yet to be Live applications. The count is already considered in application count which is 100-120.
47	Page no.6, Point no. 19	Audit of NoSQL and RDBMS Databases - Kindly elaborate more on this. What are the in-scope activities for this ?	Configuration Audit
48	Page no.6, Point no. 15	Black box (unauthenticated) or Grey box (authenticated) scan to be performed or only audit / review is to be conducted ?	Will be discussed with the successful bidder.

49	Page no. 11	IT Infrastructure in scope ?	The IT infrastructure pertains to Servers and N/W devices at DC& DR.
50	Page no. 15	One hard Copy of the masked Commercial Bid is to be submitted by the bidder. Kindly elaborate upon means of masking hard copy of the commercial bid.	No amount should be mentioned in the hard coppy of Technical Bid. Amount should only be mentioned in the Commercial Bid.
51	Page no. 43	Commercial BID is to be submitted inclussive of GST or Exclussive of GST component ?	excluding GST
52	Page no. 43	Please confirm whether Bidder can add and specify any other cost heads missing as per the commercial BID format provided ?	Yes
53	Page no. 63	The count 100-120 is overall? And all of these application needs to be tested quarterly? If not please specify the count for each quarter activity.	All these applications needs to be tested within the project timeline which is 7 months
54	Page no. 64	No. of HLD and LLD to be reviewed?	HLD and LLD not mentioned on Page 64 of RFP.
55	Page no. 70	Review/verification of compliance requirements as specified in the PCI-DSS certification standard is to be conducted for RRBs as well ? If Yes, Do VAPT for cardholder data environment should also be in scope for a selected bidder ? This will be applicable onlt to Central Bank of India (CBI) or to CBI and RRBs of CBI both ?	No, this assessment is to be carried out for Central Bank of India Only.
56	Page no. 106	Is it the complete set of DC / DR infrastructure In scope ? Do Bidder has to include any additional infrastructure in actual ?	Complete set of DC/ DR infrastructure is included in scope
57	72	No. of Server for configuration review?	there are 2000 Servers and VMs
58	72	No. of network devices for configuration review?	There are 350 no of Network devices approximately

59	72	We understand all the MBBS documents are present with bank and no further documentation is required to be prepared.	MBLS document will be provided by the Bank
60	72	Bidders are allowed to use the opensource tools to perform configuration review.	Only Licensed version tools are allowed.
61	5 and 47	Please confirm application audit count is 59 or 100-120?	100-120
62	5 and 47	We understand the VAPT needs to be performed once in 2024-25 and twice in 2025-26. Hence the total count of application will become (110+110+110=330). Please confirm if the understanding is clear.	110 applications to be audited once in 2024-25 110 applications to be audited twice in 2025-26
63	48 and 72	Please confirm the count of the API is 1000 or 250?	1000 approximately
64	98	Please provide the count for VA and PT activity, for RRB	Same as Central Bank of India
65	98	Application Review Scope - The application 27-25 needs to be tested how may times in two year?	Same as Central Bank of India
66	106	No. of devices for Vulnerability Assessment	Around 2000 servers including VMs which will increase by 15% in next two years.
67	106	No. of devices for Configuration review activity,	On sample basis
68	128	Configuration of all Network Equipment installed at DC, DRC & should be verified for any Security threats. -- Please confirm Number of devices and frequency.	there are 350 network devices approximately
69	NA	Is the usage of commercial tools is expected? If yes, tools will be provided by Bank or bidder has to consider extra cost.	It should be the part of commercial submitted.

70	Various applications under CentNeo platform as & when it goes Live during the Audit period	Request you to kindly confirm the detailed scope and expectation from this activity	At present Cent Neo is having 9 application which includes Live or yet to be Live applications. The count is already considered in application count which is 100-120.
71	Application Bug finding through automated tool.	Request you to kindly confirm the detailed scope and expectation from this activity	Auditor is expected to scan the application through some tool for finding the bugs in the application.
72	Apsec audit of Mobile applications	Request you to kindly confirm the total count of mobile apps in scope	15
73	DAST and SAST of container images	Request you to kindly confirm the total count of container images in scope	No. 17 cluster and 260 nodes
74	Audit of NoSQL and RDBMS Databases.	Request you to kindly confirm the total count of databases in scope. Also confirm if secure configuration review of database is to be performed	Will be shared with successful bidder.
75	Audit of VMWare, Nutanix, Microsoft Hypervisor, Openshift Container platform.	Request you to kindly confirm the total count of mobile apps in scope	configuration audit of Hypervisor, Container
76	Network / Cyber Security Audit:- Network Infrastructure and Security Audit of entire Network infrastructure. Audit of effectiveness of Anti-virus system.	Request you to confirm the anti-virus solution deployed in the organisation for which effectiveness review is to be performed	Trend Micro
77	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).	Please confirm the details of the scope of work under complete review of applications and security audit? Does this imply, application functionality (automated business controls), controls around access, change, backup, restoration, capacity, infrastructure management, etc?	Yes overall application security assessment is to be performed
78	Integrated Call Centre	What is the scope expectation for this line item? Do we need to perform IS Audit for the applications used by the call center?	Same as other application. Yes

79	The scope of IS audit should encompass a detailed examination of the change management process validating that any IT environment changes are business justified, documented, and subject to a robust change management protocol. Such audits should be conducted by April 30 of a Financial Year, to ensure the robustness of the change management framework and effectiveness of oversight over vendors managing critical application.	Does the statement imply that change management as part of IS audit is to be completed by 30th April 2024, for all in-scope areas? Why is this process called out specifically?	Audit of change management process of IT environment changes is to be completed by April 30 of FY as per RBI advisory.
80	Audit of ATM Project: - Security audit of ATM switch, ATM card related operations. Compliance to RBI Master Direction on Digital Payment Security Controls dated 18-Feb-2021 for Card Data & Switch environment. Compliance review of PCI-DSS standard requirements.	Request you to confirm the expectation from Compliance review of PCI-DSS environment	Assessment of Card data & Switch Environment as described in RBI Master Direction on Digital Payment Security Controls dated 18-Feb-2021 and PCI-DSS standard
81	Copy of letter of assignment & certification of satisfactory completion of assignment to be submitted from respective Bank/banks	Request you to revise the statement as below Copy of letter of assignment or certification of satisfactory completion of assignment to be submitted from respective Bank/banks	Not possible
82		Is it one time audit or will it include compliance audit/ revalidation/ retesting	It will include compliance assessment too