

CORRIGENDUM - 2 - Bank Reply to Bidders queries.

27.06.2022

Annexure

Central Bank of India: Corrigendum : Tender Reference: CO:DIT:PUR:2022-23:358 dated 16.06.2022 for commercial bids from Empanelled Auditor for conducting Vulnerability Assessment and Penetration Testing of various Applications in Central Bank Of India and It's Two RRB's - Corrigendum 1 dated 24.06.2022

Bidder	#	Subject heading	RFP Text	Query	Bank Reply
KPMG	1	Scope		Is this a one time activity for the scope mentioned in the Tender document or 2 times for 2 quarters? (April to September - there will be 2 quarters so please confirm if this will be one time activity or 2 times in Apr to Sept period.)	As per Tender, it is one time activity (Apr to Sep 2022)
	2	Timelines		As per the timelines, the activities need to be completed within 1 month (4 weeks), please confirm if there is any hard timeline to complete the activities or it can be extended.	No Change
	3	Web app		Out of 53 Apps, please provide the bifercation with the count of small, Medium and large applications.	Bank classifies applications on the basis of its criticality.
	4	General		What all activities will be carried out from Bank location?	Yes
AKS	1		Rs.1,000/- (Rupees One Thousand only) in the form of Demand Draft issued by a Scheduled Commercial bank (except Central Bank of India) in favour of "Central Bank of India" payable at Mumbai and the DD should be submitted along with the Commercial Bid. The tender fee can also be submitted by way of NEFT in account no. 3287810289 of Central Bank of India (IFSC Code – CBIN0283154) with narration "Tender ref no "CO: DIT: PUR:2022-23:358 dated 16.06.2022" in favor of "Central Bank Of India" and payable at MUMBAI	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	Exemption will be provided as per eligibility and Governemnt of India guidelines. Bidder to ensure submission of valid certificate.
AQM	1	Scope of the Job, Point no. 2	Check if any Vulnerability exists in the Servers, Database, Applications, Network and Security devices in scope without disturbing operations.	Count of the devices	As per Tender Document and Corrigendum
	2	Scope of the Job, Point no. 2 of 2	Attempting to guess passwords using password-cracking tools.	Does the Bank provide the tools or we need to arrange and configure	Bank will not provide any tool, bidder has to arrange for required tools.
	3	Scope of the Job, Point no. 7 of 2	To ascertain the configuration, placement and deployment of IDS is configured for intrusion detection, suspicious activity on host are monitored and reported to server, firewall and IDS logs are generated and scrutinized	We may need to access the infra for generating reports. Bank would provide the same.	Necessary access will be provided within intranet on case to case basis.
	4	Vulnerability Assessment- Para 1	To identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system through a variety of automated tools combined with manual verification of identified issues	Is the Bank open for using opensource tools, where we use hybrid (Open Source + Licensed ones)? Or we need to use only Licenced ones?	Open sourced can be allowed. However bidder should ensure/certify that it is free from vulnerability
	5	Penetration Testing - Para 1	To identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components through manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.	Is the Bank open for using opensource tools, where we use hybrid (Open Source + Licensed ones)? Or we need to use only Licenced ones?	Open sourced can be allowed. However bidder should ensure/certify that it is free from vulnerability
	6	4.17. Project Completion Time	Annexures which list the devises and apps for testing - time lines (4 weeks from the date of the PO) - 2 RRBs of CBI	Only VA and no PT mentioned in the RFP Also can the security testing be performed offsite- partially / fully etc.. (since the timelines are very aggressive) - in case to be done onsite, G17what are those activities for onsite location/s for testing	VA for all systems (Applications) and PT for Internet Facing Applications. Bank has DC setup at Mumbai and DR setup at Hyderabad. Bidders has to conduct VAPT of all Servers / Applications from DC Location.