



CERISMA (PRIVATE) LIMITED

PAGE

1	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED		
	ON (Date)	16.04.2026	BY (Time)

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
1	<u>IT and System Audit</u>	<u>CERISMA - HeadOffice</u>				
1.01	<u>IT & System Audit</u> System Audit		EA	1		
1.02	<u>IT & System Audit</u> VAPT		EA	1		
=====						
<p>Terms and Conditions:</p> <p>Introduction:</p> <p>Cerisma (Private) Limited is a private limited Company registered under section 16 of the Companies Act, 2017 (XIX of 2017). Cerisma Private Limited (the Company) is a wholly-owned subsidiary of Pakistan State Oil (PSO) that has been granted Pilot approval from the State Bank of Pakistan (SBP) to operate as an Electronic Money Institution (EMI).</p> <p>Instructions to Bidders:</p> <p>The selection of a company/firm will be based on Single Stage two envelope bidding procedure. The bidders are requested to examine all instruction mandatory technical evaluation criteria-<>> techno-commercial evaluation criteria and terms and conditions of the bidding documents.</p> <p>The bid shall comprise a single package containing two separate envelopes (as mentioned in SAP ARIBA). Each envelope shall contain separately the financial proposal and the technical proposal. Initially, only the envelope marked "TECHNICAL PROPOSAL" shall be opened.</p> <p>The envelope marked as "FINANCIAL PROPOSAL" shall be retained in the</p>						



CERISMA (PRIVATE) LIMITED

PAGE

2	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED			
	ON (Date)	16.04.2026	BY (Time)	

Please quote your best price for all items of following specifications. Please read the instructions attached herewith **EARNEST MONEY %** Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	<p>system. The technical proposal will be evaluated as per the technical evaluation criteria, without reference to the price and reject any proposal which does not conform to the specified requirements. Cerisma reserves the right to request submission of additional information from the bidders to clarify/further understand aspects of technical proposal, if required. After the evaluation and approval of the technical proposal the procuring agency, shall at a time within the bid validity period-<> ,<> publicly open the financial proposals of the technically accepted bids only. The most advantageous bidder will be ascertained based on technical qualification and lowest commercially evaluated bid.</p> <p>Conditional or incomplete bids will result in rejection of bids. Cerisma reserves the right to request submission of additional information from the bidders to clarify/further understand aspects of technical proposal, if required. Cerisma also reserves the right to verify any information provided by the bidder.</p> <p>Cerisma has the right to visit business premises to verify the information shared in tender documents. Bidder presenting information intentionally incorrectly or fraudulently will be disqualified. Bidders who fail to submit complete and attach all the relevant documents shall be disqualified. No bid shall be accepted in hardcopy. Bidders to strictly ensure that their bid documents are submitted before the closing time and date of the tender, else the system will not accept the bids after the closing time. CERISMA may reject all bids or proposals at any time prior to the acceptance of a bid or proposal. CERISMA shall upon request communicate to any bidder the grounds for its rejection of all bids or proposals but shall not be required to justify those grounds.</p> <p>Independence and Conflict of Interest</p> <p>The Bidder must be independent of the Company in accordance with the Code of Ethics issued by the Institute of Chartered Accountants of Pakistan.</p>					



CERISMA (PRIVATE) LIMITED

PAGE

3	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED		
	ON (Date)	16.04.2026	BY (Time)

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	<p>The Bidder shall be ineligible if it, its network firms, or personnel have provided or are providing services (including internal audit, system implementation, or advisory) that may result in a self-review or other independence threat, including auditing systems or controls previously designed, implemented, or reviewed by them.</p> <p>The Bidder shall submit a declaration of independence and conflict of interest, disclosing all relevant past and present engagements, and shall promptly notify any conflict arising during the process. The Company reserves the right to disqualify or terminate the engagement in case of any actual or perceived conflict.</p> <p>Scope of work:</p> <p>CERISMA Pvt. Ltd. seeks proposals for an IT audit to assess the security, compliance, and operational effectiveness of its platforms, including Open Wallet, Open Connect, Digital Banking Backend, Digital Banking App, Open CMS, and Open MMS. The audit must evaluate compliance with the following relevant regulatory standards: SBP#s EMI Regulations, SBP Cloud Outsourcing Framework, and industry best practices.</p> <p>CERISMA Pvt. Ltd has outsourced the aforementioned services to its technology solution partner M/s Paysys Pvt Ltd. The schedule of the audits, will be agreed mutually between the Company and the successful bidder. The key areas in scope include:</p> <p>1.#IT#Governance##Strategy ##Review of: #o#IT#organisational structure, roles, and responsibilities #o#IT#strategy alignment with business objectives #o#Policy and procedure documentation ##Verify alignment with recognised standards: #o#ISO/IEC#27001:2022 (information#security baseline) #o#NIST Cybersecurity Framework#v1.1 #o#COBIT#2019 (governance & control objectives)</p> <p>2.#IT#Infrastructure##Operations o#Evaluate servers, networks, storage, and data#centre management.</p>					



CERISMA (PRIVATE) LIMITED

PAGE

4	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED			
	ON (Date)	16.04.2026	BY (Time)	

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	<p>o#Assess the design and architecture of the system#including hardware, software, and network components</p> <p>o#Evaluate the change#management, incident#management, and service#management processes.</p> <p>o#Review backup and disaster#recovery planning.</p> <p>o#Confirm configuration compliance with CIS Benchmarks.</p> <p>o Validate immutable / air#gapped backups and evidence of at least one successful annual DR fail#over test meeting documented RTO/RPO targets.</p> <p>o#Assess deployment and effectiveness of an EDR/XDR platform mapped to MITRE#ATT&CK.</p> <p>3.#Cybersecurity#Controls</p> <p>##Network and perimeter security (e.g., firewalls, IDS/IPS)</p> <p>##Endpoint security and antivirus solutions</p> <p>##Access controls, identity, and privilege management</p> <p>##Cybersecurity awareness and training programmes</p> <p>##Physical and environmental security (relevant to cybersecurity)</p> <p>##Patch management</p> <p>##Secure remote access (e.g., VPN, Zero#Trust Network Access)</p> <p>##Secure configuration and hardening of systems</p> <p>##Data#loss#prevention (DLP) solutions</p> <p>##Email security (anti#phishing, spam filtering, DMARC/DKIM)</p> <p>##Mobile#device and BYOD security controls</p> <p>##Assess implementation of an enterprise Zero#Trust architecture (identity#centric segmentation, least privilege, continuous verification).</p> <p>4.#Data#Integrity</p> <p>##Data classification and handling</p> <p>##Encryption controls</p> <p>##Compliance with relevant data#protection laws and standards</p> <p>##Data#validation checks across the transaction lifecycle</p> <p>##Verify end#to#end encryption (TLS#1.3, AES#GCM#256#bit) for data in transit and at rest.</p> <p>##Ensure cryptographic hash#based data#integrity checks across each transaction stage.</p>					



CERISMA (PRIVATE) LIMITED

PAGE

5	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED			
	ON (Date)	16.04.2026	BY (Time)	

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	5.#Application#Security ##Secure#development#lifecycle practices ##Web#application and API security ##Patch and vulnerability management #Review SDLC documents and confirm they follow OWASP#SAMM (secure#by#design) 6.#Performance#Testing ##Verify performance and reliability under various loads and assess response to peak traffic or high transaction volumes. ##Include volumetric DDoS stress tests and chaos#engineering fault#injection scenarios to prove resilience. 7.#User#Access#Management ##Onboarding/off#boarding processes ##Multi#factor authentication and password policies ##Role#based access controls ##Privileged#access management (vault/JIT elevation, session recording) ##Quarterly access#recertification and segregation#of#duties review 8.#Compliance##Risk#Management ##Compliance with applicable regulatory requirements ##Risk#assessment and treatment processes ##Security awareness and training programmes ##Incident response and recovery ##Risk#mitigation strategies and preventive measures ##Data#Protection Impact Assessment (DPIA) process for all new high#risk data#processing activities (aligned to ISO#27701) 9.#Third#Party##Cloud#Security ##Vendor#risk management ##Cloud#infrastructure and application security ##SLAs and third#party compliance #Each cloud provider must give an independent security audit report (e.g., SOC#2 or ISO#27017). 10.#Continuous#Security#Monitoring ##Ongoing regulatory compliance ##Security#patch management					



CERISMA (PRIVATE) LIMITED

PAGE

6	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED		
	ON (Date)	16.04.2026	BY (Time)

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	<p>##Data#protection and privacy</p> <p>##Incident#management drills</p> <p>##Business#continuity and disaster#recovery testing</p> <p>##log retention of 12#months hot / 5#years cold in tamper#evident storage.</p> <p>##evidence of semi#annual threat#hunting exercises with documented remediation.</p> <p>NEW-PAGE</p> <p>11.#Vulnerability#Assessment##&#Penetration#Testing</p> <p>The service provider should perform Vulnerability Assessment and Penetration Testing Services external and internal for the critical systems and its allied components including the Core Payment Processing system and relevant Middleware etc.</p> <p>The Service Provider shall provide automated, manual or hybrid penetration testing Services, as requested. Cerisma may request the consultant to perform various types of penetration testing Services which cover (Black / Grey / White Box) Box testing. The purpose of this activity is to attempt to identify and exploit vulnerabilities and demonstrate the impact of those vulnerabilities in terms of successful attack scenarios against in-scope applications, with one-cycle of revalidation after cooling-off period in which Cerisma will remediate the vulnerabilities.</p> <p>Ensure that security testing is conducted while taking into consideration various scenarios and threats that are unique to cloud services including but not limited to hypervisor jumping, weak application programming interfaces, DoS hyper jacking, wrapping attacks, cloud malware injection, side channel attacks, etc.</p> <p>Service provider should assess the security of the entire network and databases (related to the critical systems) to confirm that the systems are able to protect from different threat vectors. These threat vectors may be from inside or outside the organization.</p> <p>.,,iOS Application</p> <p>.,,Android Application</p> <p>.,,APIs</p> <p>.,,Database</p>					



CERISMA (PRIVATE) LIMITED

PAGE

7	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED			
	ON (Date)	16.04.2026	BY (Time)	

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	.,Network components .,Servers with HA Key Areas to be Reviewed: .,External and internal security review and assessment of critical systems. .,Evaluation of network security. .,Verification of defenses against internal and external cyber threats. .,Ensure compliance verification for mobile banking apps against OWASP Mobile Top 10 .,Ensure compliance with SBP Framework on Outsourcing to Cloud Service Providers # 16 Jan 2023 .,Pen#testing team must include certified professionals (CREST, OSCP, or equivalent) to guarantee testing quality. .,Set a remediation SLA: Critical issues fixed within#15#days and High issues within#30#days, followed by mandatory retesting and evidence submission. 12.#Monitoring,#Logging#&#Incident#Response Review ##SIEM and log#management ##Incident#response planning and execution ##Forensics capabilities ##Verify SIEM detection use#cases mapped to MITRE#ATT&CK and reviewed quarterly. NEW-PAGE 13.#Methodology .,The audit team will submit a detailed phase wise methodology within first week of award of contract. .,The audit will follow a risk-based approach, prioritizing areas of higher risk and potential impact on transaction integrity and fraud prevention. The audit team may use recent cases as test case for better control measures applicability .,The audit team will conduct interviews, documentation reviews, and technical testing to assess controls and identify weaknesses. .,Technical testing may include vulnerability scanning, penetration testing, and social engineering simulations to assess the system's resilience against cyber threats.					



CERISMA (PRIVATE) LIMITED

PAGE

8	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

<p>Company PSO Dummy Vendor PAKISTAN</p>	<p>QUOTATION REQUIRED</p>			
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">ON (Date)</td> <td style="width: 50%; text-align: center;">16.04.2026</td> <td style="width: 25%;">BY (Time)</td> </tr> </table>	ON (Date)	16.04.2026	BY (Time)
ON (Date)	16.04.2026	BY (Time)		

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	<p>.,Each audit activity must be mapped to relevant standards or regulations (e.g., ISO#27001, NIST#SP#800#53, PCI#DSS#v4.0, SBP guidelines).</p> <p>##Auditors will collect objective evidence#such as screenshots, configuration extracts, and log samples#during fieldwork to demonstrate control effectiveness.</p> <p>14.#Reporting</p> <p>.,A comprehensive audit report will be prepared detailing the findings, conclusions, and recommendations resulting from the audit.</p> <p>.,A comprehensive VAPT report will be prepared detailing the findings, conclusions, and recommendations resulting from the audit.</p> <p>.,MIS report with the historical data for the vulnerabilities identified and resolved during the tenure.</p> <p>.,Risk assessment report for the identified vulnerabilities and gaps.</p> <p>.,The report will be presented to CERISMA, highlighting areas of concern and providing actionable recommendations for improvement.</p> <p>.,Follow-up on audit recommendations:</p> <p>o,,Findings will be classified as Critical, High, Medium, or Low using CVSS#v4.0 scores.</p> <p>o,,Each finding shall be cross#referenced to the relevant standard or regulation (e.g., ISO#27001 clause, NIST#SP#800#53 control, SBP guideline) for clear traceability.</p> <p>15. Payments</p> <p>I. Bid price shall be inclusive of all taxes, duties, levies, charges, etc.</p> <p>II. Bidder should quote in PKR</p> <p>III. All payments will be made in Pak Rupees.</p> <p>IV. The prices charged by the successful bidder for the required equipment/services along with accessories and associated services shall not vary from the prices as quoted in the financial proposal.</p> <p>V. Payment will be made on submission of invoices duly verified in all respect by the user Division / Department.</p> <p>VI. The most advantageous bidder will be selected based on the evaluation criteria mentioned in the document.</p> <p>16. Renewal</p>					



CERISMA (PRIVATE) LIMITED

PAGE

9	OF	9
RFQ No	CRZ0011AA	
DATE	01.04.2026	

REQUEST FOR QUOTATION

(THIS IS PRICE ENQUIRY-NOT AN ORDER)
SAP No.6100016295

Company PSO Dummy Vendor PAKISTAN	QUOTATION REQUIRED		
	ON (Date)	16.04.2026	BY (Time)

Please quote your best price for all items of following specifications. Please read the instructions attached herewith EARNEST MONEY %
Rs. _____ PO/DD NO. _____

Title: Tender for System Audit and VAPT

S.No.	Description/Specifications	Location	Unit	Qty	Unit Price Rs.	Amount Rs.
	The service order is for 1 year. The contract will be renewed in subsequent years for a total period of 3 years. To be renewed annually after mutual consent of both parties and on satisfactory performance of the vendor. Annual renewal shall be adjusted based on inflation, using the 12-month average Consumer Price Index (CPI) published by the Pakistan Bureau of Statistics. Any annual increase shall be capped at the maximum of 10%. No adjustment shall be applied during the initial contract term of 12 months.					