CITIZENS BANK PLC

Information & Communication Technology Division
Chini Shilpa Bhaban-2,76- Motijheel C/A
Dhaka-1000

Request For Proposal

Selection of a Service-Provider for conducting Vulnerability Assessment and Penetration Testing Services for the Web Applications and IT Infrastructure deployed at Citizens Bank's DC & NDC.

Submission Deadline: August 08, 2023, by 03:00 PM

1. Introduction

Citizens Bank PLC (সিটিজেনস ব্যাংক পিএলসি) is one of the fifth-generation banks, scheduled 61st Private Commercial Bank in Bangladesh. The bank started its commercial banking operations on July 03, 2022. After launching, the bank is continuing its business with a total of six branches (Principal Branch Motijheel, Gulshan Corporate Branch, Narayanganj Branch, Nayanpur Bazar Branch Kasba, Seedstore Bazar Branch Valuka, and Sonakanda Branch Keraniganj). The Bank intends to invite sealed proposals from eligible Vendors/Bidders for Vulnerability Assessment and Penetration Testing services for the Web Applications and IT Infrastructure deployed at Bank's DC & NDC.

2. Scope

This document constitutes a formal Request for Proposal (RFP) for the Selection of a Service-Provider for conducting Vulnerability Assessment and Penetration Testing Services for the Web Applications and IT Infrastructure deployed at Citizens Bank's DC & NDC.

Vulnerability Assessment and Penetration Testing should cover the web application and its components including a web server, app server, DB server, Mobile applications, networking systems, security devices integration with other applications and APIs, etc.

The selected bidder should carry out an assessment of Threats & Vulnerabilities assessments and assess the risks of the Bank's Information Technology Infrastructure. This will include identifying existing threats if any and suggesting remedial solutions and recommendations of the same to mitigate all identified risks, with the objective of enhancing the security of Information Systems. In addition to the remote Assessment, the selected Bidder shall also perform the onsite assessment of the assets under the Scope of the RFP.
After the VAPT assessment and the vendor will submit the report to the Bank, Bank may at its discretion request in writing for Compliance verification.
The frequency for conducting VAPT should be half-yearly. However, the Bank at its own discretion can change the frequency.

3. Bidder Qualifications:

- The bidder should be a company registered and working in Bangladesh.
- The Bidder should have at least three (03) years of experience providing ITES services/System Integration/ Cybersecurity/Computer Forensic and VAPT.
- The Bidder shall have its own office and adequately trained and experienced manpower to operate VAPT services.
- Bidder resources must have experience in Web Application Security Testing, Mobile Application Security Testing, Network, Firewall, and Systems or Infrastructure Security Testing.
- Bidder must have two CEH-certified professionals on staff, one CEH Practical, and one CEH master.
- The bidder shall not be under a declaration of ineligibility for corrupt, fraudulent, collusive, or coercive practices.
- Bidder must have certified professional engineers/experts like CC, CISSP, CISA, CISM, CRISC, OSCP, ISO:9001, CDCP, ITIL, CSA, CCNA, RHCSA, CPISI, etc.
- Bidder should have a minimum of four (04) existing customers (preferably in the financial sector) for similar products/items and a copy of such work order(s) must be supplied along with the tender bid as proof of experience.
- The bidder cannot outsource the resources or services to any organizations or individuals.

4. Tender Submission Method:

Technical and Financial proposals should be submitted by the bidder in separate envelopes signed and sealed by the authorized personnel of the bidder. **Technical Offer will contain exhaustive and comprehensive information about the proposed service and details of the Bill of Material & Services without pricing, whereas the Financial Offer will contain the details of item-wise price breakup & Services with pricing information.**

SUBMISSION ADDRESS OF THE PROPOSAL:

Executive Vice President &
Head of ICT Division
Citizens Bank PLC
Chini Shilpa Bhaban-2
76, Motijheel C/A, Dhaka-1000
SUBMIT THE SEALED PROPOSALS INTO THE TENDER BOX.

5. Deliverables with Bidding Documents:

The following documents must be submitted with other bidding documents:

S/N	Document Descriptions	Bidder Response
1	Company Profile	
2	Experience Certificates	
3	Work orders	
4	Income TAX Certificate	
5	Valid VAT Registration Certificate	
6	Valid Trade License	
7	Details of client list	
8	Details of certified professionals/engineers/experts	
9	Description of their support team with the profile of experts	

6. Evaluation Methodology:

The technical evaluation will be done on the basis of the information provided along with supporting documents. The proposal will be evaluated by the Bank's existing technical committee. The technical committee will review and score (if needed) all proposals and will make the final recommendation to the Bank's existing Purchase Committee.

The Board of Directors of the Bank will receive the recommendations from the Purchase Committee and make the final decision.

Evaluation Criteria

The evaluation of the Technical Bid will be based on the weightage for each Component as per the following technical Marking criteria:

Sl	Criteria	Marks
1	Minimum 3 years of experience in vulnerability assessment and penetration testing of at least 4 (four) Banks/NBFIs.	15
2	Availability of sufficient high-quality vendor personnel with certifications such as Certified Ethical Hacker (CEH), CEH Practical, CEH Master, CC, CDCP, ISO 9001, CSA, CCNA, RHCSA, etc. Penetration Tester must be an Experienced White Hacker.	15
3	VAPT tools must be authentic, renowned, and licensed.	15
4	Industry-standard penetration test methods (such as OSSTM) and scanning techniques.	15
5	External Pentest location and Platform	15
6	Attack methods, scripts, and techniques process	15
7	Legal Documents	10
	Total Marks =	**100**
	Qualify Marks =	**70**

The bidders, **who secure a minimum of 70 marks** would be considered for the subsequent financial evaluation.

The successful bidders at the end of the technical evaluation process will be considered for financial evaluation. The evaluation of the finances will be as follows:
The points/marks for the other successful quotes will be computed as per the following formula:
Financial Bid = (Lowest Bid ÷ Bidder's Price) × 100.

7. Prices, Currency, and Payments

a) Bidders shall submit their quotations for having the works under the RFP in the Offer to be filled in completely with all rates and amounts in Bangladesh currency.

b) Payments will be made as follows in Bangladeshi currency (BDT).

8. Customs Duties, VAT, IT, and Taxes

The quoted price should include all costs including Customs Duty, Sales Tax, Import Permit fees, Surcharges, VAT & income taxes.

CITIZENS BANK PLC

9. Acceptance and rejection of Tender

Non-compliance with the pre-conditions set forth herein above will lead to cancellation of tender and the Bank reserves the right not to accept the lowest tender as well as to accept or reject any or all tender without assigning any reason thereof.

10. Availability of Tender Schedule

The tender schedule will be available at ICT Division, Head Office, Chini Shilpa Bhaban-2 (Level-2), 76, Motijheel C/A, Dhaka-1000 during office hours from **24.07.2023 to 08.08.2023**.

11. Pre-Bid Meeting and Amendment

A pre-bid meeting will be held on **01.08.2023 at 11:00 AM** at ICT Division, Head Office, Chini Shilpa Bhaban-2 (Level-2), 76, Motijheel C/A, Dhaka-1000. The Bank will issue the amendment of this document by **04.08.2023** if any error(s) is/are detected and informed to the bank in writing through mail/hard copy by any bidder(s) within **03.08.2023.**

TERMS AND CONDITIONS

1. The offer will be received up to **3:00 pm on 08 August 2023** and technical offer(s) be opened at **4:00 pm on the same day** in the presence of the intending bidders or their representatives (if any) at the ICT Division, Level-2, Citizens Bank PLC, Head Office, Chini Shilpa Bhaban-2, 76, Motijheel C/A, Dhaka-1000. If the Tender cannot be opened on the scheduled date and time due to unavoidable circumstances, the same will be opened on the next working day at the same time.
2. Technical and Financial/commercial offers must be submitted in separate sealed envelopes mentioning **"Selection of a Service-Provider for conducting Vulnerability Assessment and Penetration Testing for the Web Applications and IT Infrastructure deployed at Citizens Bank's DC/NDC."**.
3. **Vendors not having a valid VAT registration number will be considered disqualified** and necessary VAT, TAX & AIT as applicable Govt. rules shall be borne by the selected bidder(s). Without the authentication of the VAT registration certificate by an officer of a Bank, the schedule will not be considered for evaluation.
4. Bidder(s) will be **disqualified if the RFP** response is incomplete.
5. The bidder must submit Certified experienced personnel's CVs, capable of successful completion of the project.
6. Bidder(s) will be disqualified if the technical response in the offer is misrepresented, inaccurate or false and if the offer is submitted after the last date or time of submission.
7. The **Citizens Bank PLC** management reserves the right to cancel any bid/tender without assigning any reason whatsoever. The management is not bound to award the contract to the bidder(s) of the lowest quoted price offer.
8. Quoted Price must be included with TAX, VAT, AIT, and any kind of Govt. charges thereof.
9. Manipulation or any kind of unusual approach or failure to submit the proposal/offer within the stipulated time frame will be treated as "**Disqualification**" to **attend the bidding**.
10. Delivery Time: **To be mentioned.**
11. Mode of **Payment:**
    a. 100% payment will be made after successfully completing the VAPT services.

I/we have completely read the terms and conditions & specifications and understood the total responsibility of the job. I/we have quoted this bid taking all the said responsibility and liability.

Name of the Bidder:	Signature:
Telephone No:	VAT Registration Number:
Address:	Seal:

TECHNICAL SPECIFICATION

All the mentioned Functionalities are Mandatory and offered particulars should be by international standards. If the offered particulars are not standard, the offer may be treated as disqualified.

Technical Requirement Summary

S/N	Particulars	Quantity	Units
A	Vulnerability Assessment (VA) and Penetration Testing (PT) for the Web Applications and IT Infrastructure of DC/NDC.	1	1

TECHNICAL SPECIFICATION

S/N	Specifications	Bidder's Response	
		Complied (Yes/No)	Detailed Explanation
A.	Vulnerability Assessment (VA) and Penetration Testing (PT) for the Web Applications and IT Infrastructure of DC/NDC		
1.	**General requirements**		
i)	Bidder should identify the people, processes, and technologies that are considered in-scope.		
ii)	The bidder should provide a detailed checklist of required documentation for the purposes of the engagement.		
iii)	The bidder should perform the VAPT in DC, and NDC as per the Bank's current network architecture.		
iv)	Bidder should consider all the IP addresses of all the end devices present in DC, and NDC under the work scope.		
2.	**VAPT Activities**		
i)	Network device configuration reviews are performed through the collection and analysis of data from a sampling of network devices, such as firewalls, routers, and switches.		
ii)	Network-based vulnerability scanning of a sample of internal systems to assess systems, network devices, and applications for vulnerabilities and security weaknesses.		
iii)	Review of automated scan results with manual testing to reduce false positive results.		
iv)	Host discovery to identify live hosts on in-scope IP address ranges.		
v)	Network-based vulnerability scanning of Internet-accessible network devices for vulnerabilities and security weaknesses.		
vi)	VAPT should be comprehensive but not limited to the following activities: • Network scanning • Port scanning • System Identification & Trusted system scanning • Vulnerability scanning • Malware scanning • Spoofing • Scenario analysis • Application security testing • OS fingerprinting • Service fingerprinting • Access control mapping • Denial of Service (DoS) Attacks • DDoS Attacks • Authorization testing • Lockout testing • Password cracking • Cookie security • Functional validations • Firewall Rule base review • Server Assessment (OS security configuration) • Network device assessment • Database assessment • Website assessment (Process) • Vulnerability research & verification • IPS/IDS review • Man-in-middle attack • Man-in-browser attack		
vii)	Web application assessment should be done as per the latest OWASP guidelines including but not limited to the following: • Injection		

CITIZENS BANK PLC. Division Head

	• Broken authentication & session management • Cross-site scripting (XSS) • Insecure direct object references • Security configuration flaws • Insecure cryptographic storage • Sensitive data exposure • Failure to restrict URL access • Missing function level access control • Cross-site request forgery (CSRF) • Using known vulnerable components • Un-validated redirects & forward • Insufficient transport layer protection • Any other attacks, which are vulnerable to the websites and web applications.		
3.	**Deliverables**		
i)	The VAPT report should contain the following: • Identification of the Auditor (Address & Contact Information) • Dates and Locations of VAPT • Terms of reference • Standards Followed • Detailed outcome of the assessment		
ii)	Summary of audit findings including identification tests, tools used, and results of tests performed (like vulnerability assessment, penetration testing, application security assessment, websites assessment, etc.): • Tools used and methodology employed • Positive security aspects identified • List of vulnerabilities identified • Description of the vulnerability • Risk rating or severity of the vulnerability • Category of Risk: Very High/ High/ Medium/ Low • Test cases used for assessing the vulnerabilities • Illustration of the used cases • Applicable screenshots • Analysis of vulnerabilities and issues of concern • Recommendations for corrective action • Personnel involved in the audit		
iii)	The VAPT report should comprise the following sub-reports: • VAPT Report – Executive Summary • VAPT Report – Core Findings along with Risk Analysis • VAPT Report – Detailed Findings/Checklists • VAPT Report – Remediation of the vulnerabilities		

Financial Proposal:

SL. No	Specifications	Unit Price	Qty.	Total Price
			Total Price (Including VAT/TAX) =	
In Words:				

Annexure-I

Vulnerability Assessment (VA) and Penetration Testing (PT) Area internal and external.

Item	Description	QTY
1.	Application VAPT	11
2.	Internal IP VAPT	15
3.	External VAPT	6

End of document

CITIZENS BANK PLC. IT Division, Head Office