MEGHNA BANK

together we sail

Tender Schedule

Of

Vulnerability Assessment & Penetration Testing
For Meghna Bank PLC.

Tender Ref: MGBPLC/PROC/RFQ/Y24/4083

Version: 2.0

*The Changes are marked in Red Color.

1. Introduction

This Request for Proposal (RFP) document has been prepared solely to assist Meghna Bank PLC. in selecting a suitable cybersecurity provider for Vulnerability Assessment and Penetration Testing (VAPT) of its critical infrastructure. This document is not a recommendation, offer, or invitation to enter into a contract, agreement, or any other arrangement regarding the services. The provision of services is subject to adherence to the selection process and the agreement on appropriate documentation between Meghna Bank PLC. and any successful bidder, as identified upon the completion of the selection process.

The objective is to solicit proposals from qualified cybersecurity providers capable of delivering comprehensive security services. The selected vendor will be responsible for enhancing Meghna Bank PLC's cybersecurity posture through proactive vulnerability management and rigorous network and application penetration testing. By engaging a competent and experienced vendor, Meghna Bank PLC aims to strengthen its defenses against cyber threats and effectively mitigate risks. The goal is to safeguard digital assets, protect sensitive information, and maintain the integrity, availability, and confidentiality of systems and data in an ever-evolving threat landscape.

2. Sub-Contracting

The selected bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, services, or other obligations required under the contract without the prior written consent of Meghna Bank.

3. Request for Quotation Schedules

RFP Reference No.	Tender Ref: MGBPLC/PROC/RFQ/Y24/4083
Date of Release of Tender	September 01,2024
Last date for submitting Queries by vendor	September 10,2024
Last date for submission of response to RFP	September 22, 2024, 4.00 PM

* Any bid received by the Bank after the deadline for submission of bids will be rejected and/or returned unopened to the Vendor, if so desired.

RFP and Inquiry Response to: For any clarifications, please communicate with Mr. Nazir Ahammed, Phone +8801719406118 & Email: ahammed.nazir@meghnabank.com.bd.

Meghna Bank PLC. will attempt to respond to all reasonable queries received in the specified manner but will not answer queries received after the specified date. Meghna Bank PLC. may, at its discretion, seek additional information from any respondent after the RFP closes, and such information will form part of the respondent's response.

Tender Preparation: Tenders must be submitted in two-envelope system i.e., one Technical Proposal & one Financial Proposal mentioning Technical/Financial Proposal on the top of each envelope. These two proposals will be submitted together in a third envelope. All the envelopes should be sealed & signed.

Submitted to: Chairman, Procurement committee, Meghan Bank Ltd, Address: Suvastu Imam Square (Level-6), 65 Gulshan Avenue, Gulshan-1, Dhaka 1212, Bangladesh.

4. Scope & Deliverables of VAPT Program

4.1 Scopes of VAPT

The scope of work includes vulnerability management, external penetration testing via external IP addresses, internal penetration testing through a pool of private IPs connected to Meghna Bank's network and systems, application penetration testing, and IT employee awareness sessions on vulnerability management. The successful bidder can arrange a one-day session on Vulnerability Assessment and Management either at our premises or offline. The details regarding the session are open for negotiation based on mutual convenience. The assessment will follow guidelines from globally recognized standards such as OWASP Top 10, SANS 20, and NIST.

The following table details the scope of Vulnerability Assessment (VA) and Penetration Testing (PT) across various asset types, specifying the number of nodes to be assessed and tested for each category.

Asset type	**Number of nodes for VA**	**Number of nodes for PT**
Applications (Web, App & API)	35	20
Server	170	30
Network device	26	0

4.2 The successful bidder will be required to provide the following detailed deliverables:

Detailed Vulnerability Assessment Reports for each asset type, comprising:

I. A thorough inventory of identified vulnerabilities, categorized by severity levels (e.g., critical, high, medium, low).
II. Detailed descriptions of each vulnerability, including affected systems, potential impact, and recommended remediation actions.
III. A risk-driven, prioritized remediation roadmap that outlines actionable steps to address identified vulnerabilities, taking into account risk severity and potential business impact.

Comprehensive Penetration Testing Reports, including:

I. Detailed documentation of successful exploitation attempts, with evidence of compromised systems or data.

II. Analysis of penetration testing methodologies employed, including reconnaissance, enumeration, exploitation, and post-exploitation phases.
III. Recommendations for mitigating identified vulnerabilities, including a prioritized list, and strengthening defensive measures to prevent future exploitation.

Executive Summary Report summarizing key findings and actionable insights, featuring:

I. High-level overview of vulnerabilities discovered, highlighting critical issues and potential security risks.
II. Recommendations for improving overall cybersecurity posture, prioritized based on severity and potential business impact.
III. Executive-level insights and recommendations for key stakeholders to facilitate informed decision-making and resource allocation.

Post-testing Consultation Sessions, including:

I. Interactive session with Meghna Bank's IT and security teams to review assessment findings and discuss recommended remediation strategies.
II. Opportunity for Q&A sessions to address any questions or concerns regarding the assessment results or proposed remediation actions.
III. Provision of expert guidance and best practices for implementing recommended remediation, including a prioritized list of measures, and strengthening cybersecurity defenses.

Final Documentation Package, comprising:

I. Consolidated reports and documentation from all assessment activities, organized in a structured and easily accessible format.
II. Supplementary materials, including tools, scripts, and technical documentation used during the assessment process.
III. Comprehensive documentation of all findings, recommendations, and remediation actions, serving as a valuable reference for future security initiatives and audits.

5. Bidder Response by requirement

Functional requirement (not limited to)

Functional requirement	**Compliance response by the bidder**
Test the strength and resilience of system passwords using password-cracking methodologies.	
Ensuring the identification of misconfigurations, broken access control, Insecure Deserialization, application logic flaws, and hidden backdoor vulnerabilities within the application.	
Assess the application's defenses against SQL injection and phishing attempts.	
Identify and verify the presence of known vulnerabilities in software, particularly in web browsers and email clients.	
Evaluate the weaknesses and vulnerabilities of the operating system.	
Determine the cause of application crashes.	
Assess the possibility of injecting malicious code into the application and database.	
Evaluate the potential for spoofing and network sniffing.	
Identify any Trojan activities present in the system.	
Assess the effectiveness of all active features in the Next-Generation (NG) firewall.	
Test for vulnerabilities Including: • IP spoofing • SYN floods • Smurf attacks • Ping of Death • Man-in-the-Middle attacks • HTTP POST flooding • Shrew attacks • Teardrop attacks • Black Nurse • Peer-to-peer exploitation • NetBIOS vulnerabilities • Script kiddie methods Identify any additional attack vectors not covered above.	

6. Bidder Experience & Qualifications

6.1 Relevant Experience

Criteria	Compliance/response to be mentioned by the participating company		Documents Submitted? (Y/N) with page no.
	Yes	No	
The bidder should be a company registered and working in Bangladesh for at least 05 (Five) years and a minimum 04 (Four) Years' experience to provide VAPT service.			
The bidder should have completed projects related to VAPT minimum in 05 (Five) Scheduled Bank			
The bidder should have completed projects related to VAPT minimum in 02 (Two) NBFI			
The bidder Should have completed projects related to VAPT minimum in 02 (Two) MFS (Mobile Financial Services)			

6.2 Technical Strength

Criteria	Compliance/response to be mentioned by the participating company		Documents Submitted? (Y/N) with page no.
	Yes	No	
The Bidder may have a proficient Team Leader for this project with IT/engineering background along with CCISO/CISM/CISSP certification with minimum of 10 years of Information Security experience. Domain experience (Information Security project) with the BFSI, Conglomerate or Telecom industry is preferred. The Project Manager must have PMP certification.			
The bidder should have minimum of 02 (Two) Certified Ethical Hacker (CEH) Certification resources and 01 (One) Offensive Security Certified Professional (OSCP) Certified Resources under company payroll. Resource profile with necessary evidence need to be enclosed.			
The bidder should have experience in named common vulnerability and exploitation numbering and should own well recognized vulnerability and exploit database, Zero Day/CVE			

The bidder should mention & perform the VA with licensed tools and PT must be done manually.			
The company has to be ISO 27001 certified.			
The Bidder should provide a common platform for daily updates related to VA & PT.			

6.3 Tender Evaluation

The method of evaluation of Tenders shall follow the 'Quality and Cost Based System' (QCBS). Evaluation will be done as per the prescribed marking format mentioned in the tender document.

The weightage of evaluations of Technical and financial offers shall be 70% and 30%, respectively. The technically responsive & financially lowest bidder shall get the total marks in the financial offer among the responsive bidders, and the others shall be evaluated on relative grading. Finally, to obtain the Ranking of the Bidders, both the Technical and Financial grades shall be summed up. To be noted, the lowest bidder will not necessarily be awarded preferential consideration.

The technical evaluation matrix is given below:

SL No.	Technical Evaluation	Actionable	Marks
1	Approach and Methodology	Proposal Document	20
2	Completed 15 VA & PT engagements in Bangladesh.	Document	15
3	The company has to be ISO 27001 or equivalent certified.	Document	5
4	The Vendor Should have mentioned licensed tools named for conducting VAPT.	Document	5
5	At least 1 Consultant with 10 years of experience in Bank/NBFI/MFS/Telco/MNC Information Security or IT Audit.	Document	10
6	The bidder should have a Certified Professional in their team i. Minimum 3 (Three) nos. of resources with CEH Certified (5 Marks) ii. Minimum 1 (One) of resources with CCISO/CISM/CISSP Certification (5 Marks) iii. Minimum 1(One) of resources with OSCP Certified (5 Marks)	Document	15
Total			**70**

7. Financial Offer

Bidder should furnish the financial offer in the following format

Scope	Quantity	Price	Job Mode
Applications (Web, App & API) Vulnerability Assessment	35		Onsite
Applications (Web, App & API) Penetration Testing	20		Onsite
Network Device Vulnerability Assessment	26		Onsite
Server Vulnerability Assessment	170		Onsite
Server Penetration Testing	30		Onsite
Total Cost excluding Tax and VAT			
TAX			
VAT			
Total Cost including Tax and VAT			

Note: The bidder is responsible for rescanning and revalidating after the successful completion of the VAPT. Meghna Bank's information security team will inform the bidder about the schedule for the rescan and revalidation

8. OFFER COVERING LETTER(Technical)

The Chairman,
Procurement Committee,
Meghna Bank PLC.,
Suvastu Imam Square,
65 Gulshan Avenue, Gulshan-1,
Dhaka 1212, Bangladesh.

Dear Sir,

Re: Response to RFP No. MGBPLC/PROC/RFQ/Y24/4083

We have reviewed and understood the contents, instructions, and terms and conditions outlined in your Request for Proposal (RFP) referenced above. With this letter, we submit our proposal for conducting Vulnerability Assessment and Penetration Testing as detailed in the RFP.
Our proposal is compliant with the terms and conditions specified in the RFP and any subsequent amendments. We acknowledge and accept all terms and conditions stipulated in the RFP. Enclosed are the necessary documents comprising our complete bid package.

We understand that Meghna Bank reserves the right to accept or reject the bid in whole or in part and may annul the entire tendering process without providing reasons for such actions.

Yours sincerely,

Signature:
Name:
Designation:
Date:
Seal:

9. SELF DECLARATION BLACKLISTING

The Chairman,
Procurement Committee,
Meghna Bank PLC.,
Suvastu Imam Square,
65 Gulshan Avenue, Gulshan-1,
Dhaka 1212, Bangladesh

Dear Sir,

Re: Response to RFP No. MGBPLC/PROC/RFQ/Y24/4083

We hereby certify that we have not been blacklisted in any Central Government / Regulatory / Banking / Insurance company in Bangladesh as on the date of the RFP.

Yours sincerely,

Signature:
Name:
Designation:
Date:
Seal:

10. Experience Details

Details of VAPT assignments carried out

SL.	Name of the Client	Client segment (Organization Type)	Date of PO	Date of completion assignment	Brief Scope of Work	Name of Lead consultant	Contact person details of the client
1							
2							
3							
4							
5							

Documentary proofs are to be enclosed to substantiate the claims made.*

Date:

_____

Seal and Signature of Bidder

*Please submit copy of Client Certificate

11. Details Team members experience

SL.	Name of proposed Engagement Manager/ Proposed Team Leader/ Team Members	Prof. Qualifications	Certificated/ Accreditations	VAPT expertise, In terms of years and areas Of expertise	IT Security Expertise In terms of Years & areas of expertise	Number of similar Assignments involved in Fintech/ Banks/NBF	Detail of Tools known	Team member: Onside/ Offside
1								
2								
3								
4								
5								

Documentary proofs are to be enclosed to substantiate the claims made.

Date:

Seal and signature of the

12. Terms and Conditions:

1. The participant vendor must submit the offer in an envelope that will contain the full name and address of the participant company. The name, address, telephone number of the contact person should be mentioned in the forwarding letter submitted with the offer.
2. The bidder should be recognized as an audit and consultancy firm having experience in implementing information security policy frameworks.
3. The bidder should be a company focusing on audit & assessment and cyber security business with a minimum of 03 years of similar business experience.
4. The bidder should have had a registered office in Bangladesh for at least the last 5 years.
5. The Tender document should be submitted along with a company letterhead pad mentioning participation in the tender process duly signed by the authorized signatory.
6. Submission of declaration regarding bidder (s) has the legal capacity to enter into the contract under the applicable law of Bangladesh, and the bidder (s) shall not be barred as per the law of the land that may be subject to legal proceedings of any kind.
7. The authority of the bidder should duly sign all the pages of the tender schedule and all the offered documents.
8. The offers should have validity for at least Three (3) months.
9. Successful bidder/vendor shall have to start the work within 7 (Seven) Working days from the date of issuance of the work order after signing an NDA with the Bank.
10. The bidder should not be blacklisted by any government institution in Bangladesh or abroad. (Self-declaration to be provided).
11. The rates must be quoted in figures as well as in words. All the prices should be mentioned in Bangladesh Taka (BDT). The payment will also be made in BDT.
12. The terms of payment will be as under:
    1. 30% After Submitting the VAPT Report
    2. 30% After Revalidation Report
    3. 40% After completing the whole Project
    4. Price includes Applicable Tax & VAT
13. A photocopy of all the relevant documents should be submitted with the offer, including:
    i. Valid Trade License
    ii. TIN certificate
14. The authority of Meghna Bank reserves the right to relax, change or drop any of the terms and conditions of the schedule without any further notice.
15. Meghna Bank reserves the right not to accept the lowest Tender and to reject any Tender, part thereof, or all Tenders without assigning any reason whatsoever.

[END]