Terms of Reference for VAPT of ERP and Non-ERP Applications, Cloud Infrastructure and Network Assessment (Weighted Evaluation Method Procurement)

Version	Date	Description
1.0	27-Mar-2022	New ToR Document Author: Md Arif Hossain
1.1	30-Mar-2022	Revised ToR Document Author: Md Arif Hossain and Imran Sadik Chowdhury
1.2	04-Apr-2022	Revised and Finalized ToR Document Author: Md Arif Hossain, Imran Sadik Chowdhury & Muhammad Raquibul Hasan

1. BACKGROUND

As a people-oriented NGO, BRAC is running multiple programmes to obtain customers personal data (financial, health, social enterprise, skill development, urban development etc.) through various means (Electronically and manually).

- The operations are spread in 13 countries with a primary focus being Bangladesh, the target audience typically belongs to the marginal population from rural and urban areas.
- BRAC has 100K+ employees and 10 million+ customers
- Increasing threats of cyber-attacks, upcoming GOB regulations related to data security poses significant importance to a self-assessment of all the digital platforms BRAC adheres to its regular operation.
- BRAC typically deals magnitudes of data including organizational confidential data, end user data (Stored locally and in cloud platform).

Now, BRAC intends to engage a competent organization for the aforementioned Network and Infrastructure Assessment project to fulfil its objectives.

2. OBJECTIVE

To strengthen the security of the BRAC's network, applications and systems for any cyber threat.
This also entails, a comprehensive infrastructure security assessment comprising of – a list applications (Including web and mobile applications), network components and related infrastructure.

A partner will conduct a comprehensive security assessment (VA/PT) of a specific portion of BRAC's infrastructure.

3. SCOPE OF WORK

- **Vulnerability assessment and Penetration Testing:**

The consultant will conduct a comprehensive security assessment (VA/PT) on BRAC's mission critical assets, which are follows:

- ❖ Vulnerability Assessment and Penetration Testing of mission critical web and mobile applications and its related servers (8 ERP Modules, 10 Non-ERP Applications).
- ❖ Vulnerability Assessment and Penetration Testing of Cloud Infrastructure
- ❖ Vulnerability assessment and Penetration Testing of Network Infrastructure

To perform the task the consultant must follow the industry best practices and guidelines and perform manual VAPT. After completion of each task the consultant should submit a detail report containing the list of findings with severity ratings, impact and mitigation plan. The consultant will suggest BRAC the deadline to fix the findings and monitor it. After fixing the problem from BRAC concern department, the consultant will perform retest to ensure the vulnerabilities are properly patched.

4. DELIVERABLES

Estimation or commercials for each of the following deliverables are required:

- **Assessment**
  - Required assessment of the existing network and application infrastructure.
  - Detailed report outlining the findings from the aforementioned assessment.
- **Exercise**
  - The incumbent vendor will do the VA/PT for the aforementioned scopes.
  - After the successful conduction of the VA/PT, the incumbent vendor will submit reports with their findings.
  - BRAC will ensure all the CRTICIAL, and HIGH priority issues are resolved in the relevant scope.
  - The incumbent vendor will retest the fixes and close the issues.
- **Output**
  - Detailed list of vulnerabilities in the applications, web services and network.
  - List of recommendations to fix/ mitigate the vulnerabilities identified.
  - Severity ratings for the vulnerabilities.
  - Categorization of the vulnerabilities according to OWASP.
  - Assist relevant implementation team while fixing the identified issues.
  - Come up with a future recommendation and plan for BRAC infra-VA/PT.

5. TIMELINE

The project has to be performed within the end of March 2023. The incumbent vendor shall include its project timeline to accomplish its all deliverables (along with any sub-deliverables) successfully.

6. VENDOR QUALIFICATION

6.1. The bidder should be a company registered and working in Bangladesh for at least 03 (Three) years.
6.2. The bidder should have Valid Trade license, ETIN, VAT registration, BASIS Membership certificate.
6.3. Bidders should have performed Penetration Testing & Vulnerability Assessment, Security audit and Application Control review for at least 02 (Two) Banks, 01 (One) telecom operator, 01 (One) NBFI, 01 (One) MFS in Bangladesh. Experience/reference along with Project Completion certificate must be submitted along with its proposal.
6.4. 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.
6.5. The bidder must have at least 03 (Three) CEH professionals employed full time.
6.6. The company has to be ISO 27001 certified.

7. DOCUMENTATION

The valid proposal must be equipped with:

1. Detailed project execution plan
2. Technical expertise and skill set
3. Quotation (with man-hour breakdown)
4. Company profile (with relevant certification)
5. Company documents
6. Project references (with Project completion certificate)

8. TERMS & CONDITIONS

a. Terms & Conditions

The Financial proposal must be inclusive of VAT and Taxes, shall contain all the components relevant to perform the services mentioned herein. The proposal should consist of appropriate resource allocation-along with the senior resources and team sizing, any other professional software or tool required to perform the aforesaid activities.

Payment will be made via bank transfer with TAX and VAT being deducted as per the guidelines and policies of the Government of Bangladesh and BRAC procurement division.

In addition, the proposal must:

- ❖ Clearly state that the amount is “all-inclusive”.
- ❖ Clearly state that the contract price is fixed regardless of any changes in the cost components.

9. Payment Schedule:

Payment Terms	Deliverables
10%	After the submission of project plan
20%	After the submission of project VAPT report
40%	Upon Final Report delivery (including Presentation for Management)
30%	Retest after fix and delivering the security roadmap for the next year

Penalty Clause: BRAC reserves the right to withhold full or partial payment of an invoice if the performance is not found satisfactory and due to any incomplete delivery or breach of any confidentiality.

b. Confidentiality

I. Any confidential or proprietary information has been disclosed (whether in writing or orally) to the consultant by the client or its employees, officers or contractors relating to the business of the client including, but not limited to, any information has specifically designated by the client as confidential and any other information which should otherwise be reasonably regarded as possessing a quality of confidence or as having a commercial value in a relation to the business of the Client. the confidential Information shall include all foreground IP;

II. Any invention, rights to inventions, improvement, patent, design, process, information, copyright work (including without limitation rights in and to technical processes, systems, methods, software design, algorithms, code, scripts or other computer software), databases or topography and any other intellectual property of any nature whatsoever in any part of the world in each case whether registered or unregistered and including all applications (or rights to apply) for, and renewals or extensions of, such rights and all similar or equivalent rights or forms of protection which may now or in the future subsist in any part of the world.

III. Access to and use of confidential information shall be restricted to those employees and persons, representatives, within the receiving party's organization with a need to use the information to perform the services in order to fulfill the purpose of this agreement, if any, in connection with which the Parties have entered into this agreement.

10. SUPPORT CLIENT & LOCATIONS

BRAC is a world's no#1 NGO with local and geographical presence; hence, support must be omnipresent and must not be location dependent.

This will also cover, existing contracts and clients of BRAC to be supported as it is until any further direct contracts are drawn between the service provider and the client itself.