TERMS OF REFERENCE (ToR)

"Hiring a firm for Vulnerability Assessment and Penetration Testing (VAPT) of a2i Applications"

A. Project Description:

The Aspire to Innovate (a2i) Programme builds on the Government of Bangladesh's efforts to introduce a citizen-centric culture of innovation in civil service to improve service delivery and make services more inclusive, affordable, reliable and easier to access. This project will provide support to establish institutional mechanisms and improve accountability to accelerate SDG achievements in Bangladesh.

This project will have three components:

1. Institutionalizing Public Service Innovation and Improving Accountability
2. Catalyzing Digital Financial Services and Fintech Innovations
3. Incubating Private Sector-enabled Public Service Innovation

B. Background of the Assignment:

Bangladesh government's operations are largely supported by various web-based services as a part of digitizing Bangladesh. It involves the use of information technology, specifically the Internet based web applications and systems, to facilitate the communication between the government and its citizens. Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Government networks and critical infrastructure around the world are under a consistent state of threat. However, the nature of the threats is anything but constant. In such scenarios strengthening the security and resilience of government cyberspace-based services have become an important mission.

In order to achieve a secure and resilient cyberspace for government services in Bangladesh, it is needed to develop, implement, and maintain cyber discernibility across the eServices including D-Nothi, National Portal Framework (NPF), MyGov, etc. through continuous full range threat and vulnerability analysis, prevention of cyber-attack, incident response, resiliency, recovery policies, and activities. Development of this infrastructure will allow government to enhanced governing of critical web-based government information and contribute to gradual cyber evolution across all organization. The responsibility also extends to the organizations networks, and computer systems, whether on- premise or on the Internet while monitoring a variety of website and web-based services and tools (including the Managed Security Service, the firewalls, third party sensor/detector/rating services, internal account activity tools, and threat information services) in order to predict, detect, and diagnose threat activity, and advise, direct or participate in containment, eradication, and restoration activities in collaboration with core management team.

C. Objectives of the assignment:

The primary objective of the assignment is to protect information assets against threats and vulnerabilities, to which the organization's attack surface may be exposed. Taken together, threats and vulnerabilities constitute information risk. Ensuring that security objectives are met and risk mitigated will benefit e-services by contributing to:

- Business continuity

- Operational Efficiency
- Cost Effectiveness

An adequate cybersecurity program which will secure internal data that an enterprise considers confidential and/or proprietary, it should also protect the personally identifiable information of its customers. To safeguard each system the following security objectives can be realized,

- Confidentiality - Protecting information from unauthorized access and disclosure.
- Integrity - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
- Availability - Defending information systems and resources to ensure timely and reliable access and use of information.

The objective of VAPT is followings:

- Examine to what extent security controls are in place
- Identify deficiencies and examine the security parameter
- Identify the vulnerabilities in the systems
- Perform activity in order to exploit system.
- Conduct comprehensive VAPT across selected products.

D. Firm Qualification & Professional Competency Requirements:

To ensure high-quality and globally compliant cyber security testing, the participating firm must meet the following minimum eligibility and competency standards:

(i) Organizational Reputation & Accreditation

- The firm must have a proven reputation in the field of cyber security, demonstrated through previous engagements with government, large-scale private sector environments or banking sectors.

- The organization good to have relevant international cyber security accreditation/certification, such as ISO 27001, PCI-DSS, SOC-II, or equivalent global recognition and during the submission, **clear copy of certificate with certificate number should be submitted with proposal.**

- Prior experience in conducting VAPT of critical systems, web applications, APIs, servers, and mobile platforms will be considered an added advantage.

- The firm must ensure the ability to maintain confidentiality, integrity, and security of sensitive information related to government systems.

- In addition to the manual testing approach, the firm shall provide **the list of licensed (paid) security testing tools** that will be used for this project. The firm must **also submit proof of ownership** or valid license documentation of the mentioned tools along with the proposal.

- **Team Composition**

Team Members:

Sl. No	Position	Number of Employee
Team Members of the Software Change Management Phase:		
1.	Cyber Security Team Lead	1
2.	Project Manager	1
3.	Senior Engineer / Senior Penetration Tester (Web-application Pen-test Expert)	1
4.	Senior Engineer / Senior Penetration Tester (APK-application Pen-test Expert)	1
5.	Senior Engineer / Senior Penetration Tester (IOS-application Pen-test Expert)	1
6.	Senior Engineer / Senior Penetration Tester (Cloud & Network Pen-test Expert)	2
7.	Engineer / Penetration Tester	5
8.	Technical Document Expert	1
9.	Technical Document Writer	2

The participants organization shall submit the **Curriculum Vitae (CV)** of all proposed team members as part of the Technical Proposal. The CVs must clearly demonstrate the qualifications, competencies, and relevant experience of the personnel proposed for the assignment.

Each CV shall include, but not be limited to, the following information:

1. **Full Name of the Personnel**
2. **Current Designation and Proposed Position** in the assignment
3. **Roles and Responsibilities** in the proposed project
4. **Total Years of Professional Experience**
5. **Number of Relevant Projects Completed**
6. **Area of Expertise and Technical Skill Set** relevant to the assignment
7. **Educational Qualifications**, including degree, institution name, and year of completion
8. **Professional Certifications**, including certification name, issuing authority, year of issuance, and **certificate number**
9. **Summary of Relevant Work Experience** demonstrating suitability for the assignment

Supporting Documents:

- A **clear copy of all professional certification certificates** must be submitted along with the CV for verification purposes.

- **Project Team Members Qualification**

Team Members Schedule:

Sl. No	Position	No. of pos.	Responsibility	Qualification
1.	Cyber Security Team Lead	1	• Provide overall leadership and technical direction for all VAPT activities. • Define testing methodologies, ensure adherence to OWASP, NIST, ISO standards. • Oversee vulnerability verification, exploitation logic, PoC quality, and risk scoring. • Coordinate with a2i Cyber Security Team and ensure timely response to queries. • Validate all final deliverables, including initial and revalidation reports.	• Bachelor's degree in CSE/ICT or equivalent. • Minimum 7 years of progressive experience in cyber security and penetration testing. • Strong background in managing large-scale security assessment projects. • Preferred Certifications: OSCP, CISA, CISSP, GIAC or other intermediate/advanced certifications. • Penetration testing related certificate/qualification will be get priority first.
2.	Project Manager	1	• Plan, monitor and control all project phases from inception to revalidation. • Prepare detailed work plans, schedules, weekly progress reports, and escalation notes. • Maintain communication with stakeholders and ensure timely submission of deliverables. • Resolve administrative and coordination issues between technical teams and client. • Ensure all compliance, documentation, and contractual obligations are met.	• Bachelor's degree in CSE/ICT or related field. • Minimum 3 years' experience managing ICT or cyber security projects. • Strong communication, documentation, and client management skills. • Preferred Certifications related to project management and will get priority first.
3.	Senior Engineer / Senior Penetration Tester (Web-application Pen-test Expert)	1	• Conduct deep manual penetration testing of large-scale web applications and APIs. • Identify complex logic flaws, chained vulnerabilities, and business impact issues. • Perform exploit development, PoC demonstration, and vulnerability validation.	• Bachelor's degree in CSE/ICT. • Minimum 3 years' hands-on experience in web application VAPT. • Strong expertise in BurpSuite, proxy tools, exploitation frameworks • Preferred Certifications: OSCP, CISA, CISSP, GIAC or other intermediate/advanced

			• Follow OWASP Top 10, and ASVS checklist, NIST 800-115, and industry best practices. • Prepare module-wise findings and support the reporting team.	certifications. (intermediate level) • Penetration testing related certificate/qualification will be get priority first.
4.	Senior Engineer / Senior Penetration Tester (APK-application Pen-test Expert)	1	• Conduct Android mobile application security assessment as per OWASP MASVS/MSTG. • Perform static and dynamic analysis of APKs and associated APIs. • Identify platform-specific weaknesses, insecure storage, permissions, hardcoded keys. • Prepare detailed security findings, exploitation evidence, and remediation advice.	• Bachelor's degree in CSE/ICT. • Minimum 4 years' Android VAPT experience. • Expertise in MobSF, dynamic analysis tools, reverse engineering. • Preferred Certifications: OSCP, CISA, CISSP, GIAC or other intermediate/advanced certifications. (intermediate level). • Penetration testing related certificate/qualification will be get priority first.
5.	Senior Engineer / Senior Penetration Tester (IOS-application Pen-test Expert)	1	• Conduct iOS application penetration testing following OWASP Mobile standards. • Analyze IPA files, secure storage, keychain usage, app permissions, and APIs. • Perform jailbroken environment testing and identify broken cryptography issues. • Provide mitigation strategies aligned with Apple secure coding guidelines	• Bachelor's degree in CSE/ICT. • Minimum 4 years iOS security assessment experience. • Experience with iOS reverse engineering tools. • Preferred Certifications: OSCP, CISA, CISSP, GIAC or other intermediate/advanced certifications. (intermediate level). • Penetration testing related certificate/qualification will be get priority first.
6.	Senior Engineer / Senior Penetration Tester (Cloud & Network Pen-test Expert)	2	• Perform network, infrastructure and cloud security assessments. • Review firewall rules, server configurations, exposed services, and access policies. • Identify misconfigurations, privilege escalation vectors, weak encryption, open ports. • Conduct threat emulation across servers and cloud components. • Support the development team with hardening recommendations.	• Bachelor's degree in CSE/ICT. • Minimum 4 years' experience in network/cloud penetration testing. • Skilled in Nmap, Nessus, Wireshark, cloud security baselines. • Preferred Certifications: OSCP, CISA, CISSP, GIAC or other intermediate/advanced certifications. (intermediate level).

				• Penetration testing related certificate/qualification will be get priority first.
7.	Engineer / Penetration Tester	5	• Assist senior testers with manual testing, exploitation, and validation. • Perform scanning, enumeration, and initial analysis using security tools. • Capture PoC screenshots, logs, and maintain evidence trails. • Support initial and revalidation testing activities across all platforms.	• Bachelor's degree in CSE/ICT. • Minimum 2 years' practical experience in VAPT. • Familiarity with common security tools and manual testing methods. • Preferred Certifications: CEH, CompTIA Security+, or other entry level certifications on cyber security. (entry1 level). • Penetration testing related certificate/qualification will be get priority first.
8.	Technical Document Expert	1	• Translate technical findings into structured documents and formatted reports. • Ensure consistency, accuracy, and alignment with reporting standards. • Collaborate with security engineers for detailed remediation and risk scoring section.	• Bachelor's degree in CSE/ICT or relevant discipline. • Minimum 3 years' experience in technical documentation. • Should to have Microsoft word, excel and Power-point presentation skill.
9.	Technical Document Writer	2	• Prepare final VAPT reports, user manuals, and release notes. • Ensure clarity, readability, and professional presentation of documents. • Assist in compiling both initial and revalidation assessment reports.	• Bachelor's degree in any relevant field. • Minimum 2 years documentation experience. • Should to have Microsoft word, excel and Power-point presentation skill.

E. Scope of work:

SL	Product Name	URLs	Sub-domain	Total URLs	APK	IOS	Servers
1.	National Portal Framework (NPF) V2	3	-	3	1	1	4
2.	National Dashboard Framework (NDF)	1	-	1	-	-	2
3.	MyGov	11	-	11	2	2	4
4.	Muktopaath	2	-	2	1	-	2

5.	Ekpay	1	6	7	-	-	23
6.	A2i Dashboard	1	-	1	1	1	3
7.	A2i ERP	1	-	1	-	-	2
8.	Nothi	4	-	4	1	1	2
9.	Doptor	3	-	3	-	-	12
10.	RMS	-	-	-	-	1	-
	Total			33	6	6	54

F. Process of the project:

VAPT stands for "Vulnerability Assessment and Penetration Testing". It is a comprehensive security testing approach used to identify and assess vulnerabilities within an organization's software systems, networks, applications, and infrastructure.

Vulnerability Assessment (VA): A combination of automated and manual scan may be performed on the organization's IT systems or network, to identify flaws that may be exploited during an attack. The systematic approach of identifying, quantifying, and ranking security vulnerabilities enables organizations to select critical vulnerabilities to resolve based on the available resources. Without such assessments, there is a risk that IT infrastructure is not sufficiently secured. It is recommended that organizations should perform a vulnerability assessment on their IT infrastructure. The firm must utilize licensed (paid) industry-standard security testing tools, including but not limited to Burp Suite Professional, Acunetix, Nessus Professional/Expert, and Metasploit Pro, during the Vulnerability Assessment activities. As part of the proposal submission, the firm shall provide valid documentary evidence of ownership or active license for the tools proposed to be used in the project.

Penetration Testing (PT): To discover security weaknesses in the organization's IT infrastructure and applications, it uses an intrusive approach. The firm would attempt to exploit identified security weaknesses to gain privileged access into the IT infrastructure and applications. Such approach emulates a real attack, and would determine the robustness of the organization's IT infrastructure in protecting sensitive information. The firm must strictly adhere to recognized penetration testing methodologies. During the scanning, enumeration, and OSINT phases, the firm shall actively identify and analyze any leaked or exposed sensitive user data, system information, or other confidential information that is publicly accessible. This shall include targeted searches across open sources, breach repositories, hacker communities, underground forums, and dark-web marketplaces to determine whether any a2i-related systems, software or user data has been leaked, exposed, or sold.

Security Guideline for eService's: Individual security Guideline will be prepared for each of the eservices for Its Operational Activities and Risk Mitigation steps.

Revaluate: One (1) revalidation test to be conducted after delivery of the first VAPT report. These phases will include revalidation of fixes, assessment of overall system security, and a detailed report outlining the findings and recommendations for further improvement.

Types of Penetration Testing:

(i) In Black Box testing: the tester does not know the internal workings of the system being tested. It focuses on testing the functionality and behavior of the application from an end- user perspective. Testers typically use specifications, requirements, and design documents

(ii) Gray-Box Testing: Gray-Box Testing is a combination of both Black Box and White Box testing. Testers have partial knowledge of the internal workings of the system, such as access to the code or architecture documentation. This approach aims to simulate the knowledge an attacker
might have, while still benefiting from insights into the internal code.

G. Major Tasks to do:

a) Conduct comprehensive **black box** and **grey box** penetration tests across the agreed scope (web applications, APIs, mobile apps, servers, network segments).
b) Conduct **Red Teaming assessment** simulating real-world adversaries against agreed objectives.
c) During the enumeration phase, the team shall also assess surface and dark web sources to identify any data breaches, credential leaks, or unauthorized exposure of organization systems or user information, and report findings with evidence and recommended mitigations.
d) The firm must follow recognized penetration testing methodologies. Throughout the scanning, enumeration, and OSINT phases, the firm shall identify and evaluate any sensitive user data, system details, or confidential information that is publicly accessible. Targeted searches must include open sources, breach repositories, hacker forums, underground communities, and dark-web marketplaces to ascertain any leakage or exposure of a2i-related systems, software or user data.
e) Implement, test and operate advanced software security techniques in compliance with the client's technical reference architecture.
f) Follow industry-standard security frameworks (OWASP Top 10, NIST, etc.) in planning and performing tests.
g) Prioritize threats and high-risk assets based on impact to business objectives.
h) Work across different OS platforms and technologies to design holistic security findings and suggested mitigations.
i) Exploit identified security flaws with controlled attack simulations on agreed systems and networks in accordance with the approved scope of work.
j) Apply systems analysis techniques including stakeholder consultations to determine security specifications and constraints.
k) Research and evaluate emerging cyber threats and recommend mitigations.
l) Customize the Vulnerability Assessment and Penetration Testing report according to business context for each platform.
m) Perform **manual testing** to identify logic flaws, chained vulnerabilities, and other weaknesses not discoverable by automated tools.
n) Obtain **proof-of-concept (PoC)** for each confirmed vulnerability (screenshots, request/response captures, exploit scripts where safe) and avoid the false positive issues.
o) Analyze **impact** and **probability** for each confirmed issue and determine an appropriate **risk rating**.
p) Firm can choice of Different Tools and Software where the license cost will be paid by firms.

q) The firm shall promptly notify the a2i Cyber Security team of any critical vulnerabilities or security issues discovered during the penetration testing process. All such findings must subsequently be incorporated with detailed evidence, risk assessment, and remediation recommendations in the final VAPT report.

H. Duration of the Assignment

- **Total Duration of the assignment is 90 Days**
- Selected firm will have to sign separate SLA and Non-Discloser Agreement (NDA).

I. Reporting

Upon completion of testing, Firms will provide report as per schedule. These test reports will provide both narrative and technical details of the test and will include the following:

- Executive Summary.
- Scope of work or target system.
- Assessment Type (Initial VAPT Report / Revalidation Report).
- Summary of the Issues with impact and CVSS score.
- Issue Name or Vulnerability Title.
- Issue Details - Description of each vulnerability found and their impact. Following information will be provided for each vulnerability: Risk rating (i.e.,Critical, High, Medium, Low) and CVSS score.
- Affected item/path (i.e., URL, Website, server)
- Impact (i.e., by utilized "X" exploit, privilege can be escalated)
- Step by step attack reproduce/regenerate steps.
- Step by step remediation guideline.
- Simulated attack Proof of Concept (PoC).
- Reference of the vulnerability (example, CVE-2021-2423, CWE-123 etc.)
- Appendices containing supporting documentation (if applicable).
- In the revaluate test, New PoC will be added after the previous PoC.

The selected firm must provide **separate, individual VAPT reports for each product** included within the scope of this assignment. Each report shall be delivered as an independent document and must clearly include a title and shall be submitted in both **soft copy (PDF)** and **three (3) printed hard copies** as per the ToR requirements.

J. Standard Operating Procedure (SOP) Document

The selected firm must provide a **separate and comprehensive Standard Operating Procedure (SOP)** document along with the VAPT deliverables. The SOP shall outline the required operational steps, preventive security measures, and routine practices necessary to ensure the secure operation and maintenance of the assessed systems.

The SOP must include, at minimum:

- Standard procedures for **secure deployment, server hardening, configuration management, and patch/update cycles**.
- Guidelines on **user access control**, password policies, authentication methods, and privilege management.

- Instructions for **security log monitoring**, anomaly detection, backup and recovery processes, and encryption practices.
- Recommended **preventive security measures** for applications, databases, APIs, mobile apps, and cloud/server environments.
- A routine schedule and methodology for conducting **periodic VAPT, Security Audit, and security health checks**.
- Steps for **incident response**, escalation procedures, threat mitigation, and restoration activities.
- Any additional operational guidelines aligned with industry standards, like: (OWASP, NIST, CIS Controls, ISO 27001) etc.

The SOP must be submitted as a **separate standalone document** in both soft copy and printed form. This document will serve as the baseline reference for a2i to maintain ongoing security and operational compliance.

K. Monitoring and Engagement:

a2i Cyber Security Team will observe all project activities and continuously monitor every step of the project. The team will serve as the primary point of contact for all matters related to security, monitoring, and incident response. All project stakeholders, firms, and partners shall coordinate with the a2i Cyber Security Team for guidance, reporting, and issue resolution related to project security.

L. Delivery and Payment Schedule:

The required deliverables and payment schedule as bellows-

Sl	Deliverable	Timeline
1	**Inception and Start of VAPT** Submission of inception report with detailed work plan and commencement of VAPT activities.	End of 10 days upon the signing of the contract
2	**Detailed VAPT Report (Initial Assessment)** • Submission of the comprehensive initial VAPT report, including identified vulnerabilities, risk ratings, impact analysis, and recommended mitigation measures. • Submission of separate, individual VAPT reports for each product. • Submission soft copy (PDF) and Three (3) set of printed copy of the report.	End of 50 days upon the signing of the contract
3	**Final Report:** • After the implementation of remediation measures by the development team, a revalidation assessment will be conducted. An updated VAPT report will be submitted, reflecting verified fixes and any remaining vulnerabilities. • Submission of separate, individual VAPT reports for each product. • Submission soft copy (PDF) and Three (3) set of printed copy of the report. • Submission of a separate and comprehensive Standard Operating Procedure (SOP) document, including	End of 90 days upon the signing of the contract

	preventive security measures and operational guidelines, with soft copy (PDF) and Three (3) sets of printed copy.	

Joint Venture

Multiple Companies having technical and legal competencies for providing such services can apply jointly but they must have legal agreement among them where one company needs to be led. The joint venture company jointly needs to fulfil all conditions mentioned in this ToR. The joint-venture agreement needs to have clear identification about each responsibility matrix along with IPR. In case of JV, JV agreement as per rule 70(2), PPR 2025, Schedule 12 to be used. For JV participation, e-GP requirement for JV formation needs to be complied.