PHILIPPINE COMPETITION COMMISSION
Ensuring businesses compete and consumers benefit

25/F Vertis North Corporate Center I,
North Avenue, Quezon City 1105
www.phcc.gov.ph
queries@phcc.gov.ph
(+632) 8771 9722
(+632) 8771 9713

REQUEST FOR PROPOSAL

Consultancy Services for the Conduct of Vulnerability Assessment and Penetration Testing: Configuration and Code Review

P.R. No./Date Received: **2025-09-0145 / 12 Sept. 2025** RFQ/P No. / Date: **2025-10-0168 / 30 Oct. 2025**

The Philippine Competition Commission invites all eligible and PhilGEPS-registered suppliers, contractors and consultants to quote the best offer for the described item in the attached **Terms of Reference** subject to the Terms and Conditions and within the Approved Budget for the Contract.

Required Documents/Information to be submitted as Attachments to the Proposal:

- Valid Mayor's/Business Permit / BIR Cetificate of Registration in case of individual.
- PhilGEPS Registration Number
- Notarized Omnibus Sworn Statement
- Signed Request for Proposal
- Signed Terms of Reference
- Other documents required as basis for evaluation in the Terms of Reference

This pro-forma quotation maybe submitted through ***registered*** or ***electronic mail*** to the PCC Bids and Awards Committee (PBAC) Secretariat at above address or email to ***procurement@phcc.gov.ph*** or ***mrfajutnao@phcc.gov.ph*** on or before **05 November 2025, 1:00PM** subject to the following *Terms and Conditions:*

1. All entries shall be typed or written in a clear legible manner.
2. No alternate quotation/offer is allowed, suppliers who submitted more than one quotation shall be automatically disqualified.
3. All prices offered herein are valid, binding and effective for THIRTY (30) calendar days upon issuance of this document. Alternative bids shall be rejected.
4. Price quotations to be denominated in Philippine Peso shall include all applicable government taxes subject to **(BIR 2306)** 5% R-VAT and **(BIR 2307)** 1% (PO) or 2% (JO) deductions.
5. PCC PBAC may require you to submit documents that will prove your legal, financial and technical capability to undertake this contract.
6. Salient provisions of the IRR of RA 12009: Section 71 - Liquidated Damages and Section 98 - Imposition of Administrative Penalties shall be observed.
7. PCC reserves the right to reject any and all quotations, declare a failure, or not award the contract pursuant to Sec 70 of the same IRR.
8. In case of tie quotations, suppliers' presence are required during tie breaking through draw lots or toss coin.
9. In case supplier pro forma quotation is submitted, conditions will be governed by the submitted signed **Terms of Reference**.
10. The award of the procurement is on a **per lot basis.**
11. This project adopts the Implementing Rules and Regulations of RA 12009.

Very truly yours,

[confidential]

ATTY. JOSEPH MELVIN B. BASAS
PBAC Chairperson

[confident
ial]

Item	QTY	Unit	Total ABC	Item/Description	Total Amount (PhP) *(To be filled-out by the supplier)*
1	1	Lot	₱ 666,800.00	Consultancy Services for the Conduct of Vulnerability Assessment and Penetration Testing: Configuration and Code Review	
				(Please see attached Terms of Reference)	
Total ABC			**₱ 666,800.00**	**TOTAL Amount**	
Delivery Instructions:				*(Please see attached Terms of Reference)*	

*(Please provide **complete** information below)*

We undertake, if our Proposal is accepted, to supply/deliver the goods in accordance with the specifications and/or delivery schedule.

We agree to abide by this proposal for the price validity period specified in the terms and conditions and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Until a Purchase/Job Order or a Contract is prepared and executed, this Proposal shall be binding upon us. We understand that you are not bound to accept the lowest or any Proposal you may receive.

Signature over Printed Name : _____
Designation/Position : _____
Name of Company : _____
Address : _____
Telephone / Fax : _____
E-mail Address: _____
Company Tax Identification Number : _____

PHILIPPINE COMPETITION COMMISSION
Ensuring businesses compete and consumers benefit

25/F Vertis North Corporate Center 1,
North Avenue, Quezon City 1105
www.phcc.gov.ph
queries@phcc.gov.ph
(+632) 8771 9722

TERMS OF REFERENCE

Consultancy Services for the Conduct of Vulnerability Assessment and Penetration Testing: Configuration and Code Review

I. RATIONALE

The Philippine Competition Commission (PCC) has successfully established and approved its Information Security Management System (ISMS), which sets out internal controls and risk management measures aimed at addressing threats and vulnerabilities to ensure the protection of information.

In line with Annex A of the ISMS standard (ISO 27001:2022), specifically control A.8.8 on Technical Vulnerability Management, organizations are required to timely obtain information on technical vulnerabilities affecting their information systems, assess their exposure, and take appropriate actions to mitigate associated risks. To meet these requirements, PCC recognizes the need to engage a third-party service provider to perform Vulnerability Assessment and Penetration Testing (VAPT) on its information technology (IT) systems.

II. OBJECTIVES

1. Ensure systems compliance with ISMS (ISO/IEC 27001:2022) mandatory documented information, applicable controls, and other regulatory requirements.
2. Conduct an assessment of server configuration and code review of two applications.
3. Identify and prioritize organizational risks relative to the results of VAPT.
4. Ensure the confidentiality, integrity, and availability of PCC information assets.
5. Remediate identified vulnerabilities and recommend countermeasures.

III. SCOPE OF WORKS

The service provider shall perform the following Scope of Works (SOW) but not limited to:

1. Conduct of Pre-Assessment

    a. Recommend risk assessment methodology and address the following but not limited to: (1) baseline security criteria, (2) risk level scale, (3) risk appetite, and (4) scenario-based or asset-based risk assessment.

    b. Identify threats and vulnerabilities that apply to each application.

    c. Qualify the extent of risk and assign the impact and likelihood values of the risk occurrence

2. Conduct of Assessment for Server Configuration and Code Review

    a. **General Requirements**

I. Application – Two (2) Applications

Code Review			Configuration Review	
Application	Programming Language	No. of Lines	Database	Operating System
Application 1	Laravel	3,617,344	MYSQL	Linux
Application 2	Laravel	3,926,142	MYSQL	Linux

Note: if the application does not consume the number of lines, it can be transferred to other application to complete the required number of lines

II. Provide necessary software or tools for the conduct of the VAPT.
III. Provide documentation, reports, and a threat remediation/action plan to address the vulnerabilities discovered.

b. Scope:

I. Pre-assessment phase to determine and finalize the scope and boundaries.

II. Assessment and Capacity Building phase that complies with the full cycle of VAPT Configuration and Source Code Review. The provider must outline the tools, software/ hardware, and other peripherals that will be required to assess vulnerability.

III. Post-assessment – Submission of Final VAPT Compilation Report

3. Installation, configuration, and deployment of OpenVAS.

4. Provide training on the following:

OpenVAS and OWASP for fourteen (14) personnel covering topics but not limited to the following:

a) Introduction to Information Security
b) CIA Triad, Identity and Access Management
c) Threat Risk Modeling
d) OWASP's Role in Security Standards
e) Secure Coding Concepts
f) Input Validation, Session Management, Error Handling
g) Secure Coding Principles (Coding Standards, Secure Lifecycle)
h) Authentication and Authorization Best Practices
i) Input Filtering, Rate Limiting, Logging
j) Business Logic and Common Flaws
k) Logical Flaws, Broken Business Rules, Abuse Cases
l) Secure Web Architecture
m) OpenVAS module:
    - Introduction to OpenVAS

- OpenVAS Configuration
- OpenVAS Server Configuration
    - Step by Step of OpenVAS on Kali/Debian
    - Network and Web UI Configuration
    - Creating Secure Access Controls and User Roles
    - Tuning Performance and Storage Settings
- Architecture and Components
- Lab Setup: Import VMs, Kali Linux, Metasploitable
- Freed Update, CVSS Calculator, Legal Considerations
- Basic OpenVAS Operations
- Creating Targets and Tasks
- Running Basic Scans (Unauthenticated)
- Report Formats, Results, Vulnerability Classifications
- Advanced Task Wizard
- Authenticated Scan Steps
- Alerts and Notifications
- Network Discorvery
- Nmap Integration, Wireshark Basics
- Host Identification and Filtering
- Remediation Validation
- Role-based Access and Performance Testing
- Integrating OWASP and OpenVAS in CI/CD
- Secure Code Review Tools
- OpenVAS API/CLI usage
- DevSecOps Automation Examples
- Report Generation
- Executive Summary and Technical Details
- Prioritization and Remediation Plans
- Metasploit Integration
    - Introduction to Metasploit Framework
    - Installing and Configuring Metasploit on Kali Linux
    - Using Metasploit to Validate OpenVAS Findings
    - Common Exploits and Payloads
    - Post-Exploitation Basics and Reporting

IV. APPROVED BUDGT FOR THE CONTRACT (ABC)

The ABC for the project is Six Hundred Sixty-Six Thousand Eight Hundred Pesos Only (PhP666,800.00) inclusive of all applicable government taxes and services. The contract price shall include all the costs and profits arising from the or in relation to the services rendered in connection with the engagement and until the end of the contract.

Bids received more than the ABC shall be automatically rejected at bid opening.

V. CRITERIA FOR THE EVALUATION OF BIDDERS

The technical and financial proposals of the shortlisted bidders will be evaluated through Quality-Cost-Based Evaluation (QCBE), based on the following criteria:

Criteria	Basis
Technical Proposal (80%)	
a. Experience and capability of the firm (20%)	Records of previous engagement, quality, and extensive knowledge on the conduct of vulnerability assessment and penetration testing.
b. Applicable years of relevant experience of the firm (10%)	Experience similar or related to the project, following industry standard approach and methodology in conducting vulnerability assessment and penetration testing.
c. Quality of personnel to be assigned to the project (20%)	Submitted signed extensive curriculum vitae, certifications and years of experience in the field IT security, protection of information assets, risk management, network and application management and other computer controls.
d. Plan of approach and methodology (30%)	Timing of deliverables, qualitative and quantitative result of the assessment and threat remediation
Financial Proposal (20%)	

The bidder with the highest rated score based on the technical and financial proposals submitted, provided that the score shall pass the hurdle rate of 80 percent, shall be the Highest Rated Bidder.

VI. TECHNICAL SPECIFICATIONS

Minimum and/or equivalent functional requirements, technical specifications, features, characteristics and numbers for:

1. Team must comprise of One (1) Project Lead / Manager, three (3) Team members with expertise in server configuration and code review for applications and other computer controls.
2. Approach and methodology shall be aligned with PCC needs. The provider must take into consideration the business continuity while planning the testing of vulnerabilities identified;
3. The plan and methodology must be reviewed by the Project Manager (ICTD personnel assigned) and approved by the Chief, Information and Communication Technology Division.
4. Methodology shall be based on globally accepted standard;
5. Reports shall be industry-based correlation of vulnerabilities;
6. Must involve ICTD personnel in the conduct of the server configuration and code review and notify immediately of any critical vulnerabilities;
7. Configuration and code review shall be done on-site, with the supervision of ICTD personnel. Source codes can be reviewed within the premises of the provider and any findings and recommendations shall be kept confidential, and the provider must agree to sign a non-disclosure agreement.
8. Must provide practical, doable, and effective solution for remediation of the vulnerabilities discovered.
9. Provide all materials, equipment, and peripherals, scope of works not mentioned in this Terms of Reference but needed in the completion of the project.

VII. TIMELINES, DELIVERABLES AND SCHEDULE OF PAYMENT

The Service Provider shall be engaged for approximately forty-seven (47) days immediately after acceptance of notice to proceed of the service provider. All payments shall be certified by the Chief of Information and Communication Technology Division and approved by the Director of the Administrative Office. Each milestone payment shall be released upon PCC's acceptance of the deliverables listed. Milestone payment shall be as follows:

MILESTONES	DELIVERABLES	COMPLETION TIME	% of contract amount
Submission of workplan	Detailed Work Plan	Within five (5) calendar days after issuance of Notice to Proceed	10%
Pre-Assessment Activities Conduct of Risk Assessment	a. Approved VAPT Configuration and Code Review Methodology. b. Risk Assessment	Within seven (7) calendar days after the receipt and acceptance of Detailed Work Plan	10%
Assessment Activities 1. Conduct of Configuration and Code Review	Approved Vulnerability Assessment Matrix/Report	Within seven (7) calendar days after the completion and the PCC's acceptance of the Approved VAPT Configuration and Code Review Methodology and Risk Assessment	20%
2. Threat Remediation	Upon receipt and acceptance of the following: i. Threat Remediation Plan and Prioritization. ii. Threat Remediation Report	Within seven (7) calendar days after the completion and the PCC's acceptance of the Approved Vulnerability Assessment Matrix/Report	20%

3. Installation, configuration and deployment of OpenVAS	Submission of Installation, configuration and deployment of OpenVAS document	Within seven (7) calendar days after completion and the PCC's acceptance of the Threat Remediation Report and Threat Remediation Plan and Prioritization	10%
4. Training	Conduct of Required Training Training voucher (valid for one (1) year) may be accepted upon confirmation of the Chief, Information and Communication Technology Division	Within seven (7) calendar days after the completion and the PCC's acceptance of the Installation, configuration and deployment of OpenVAS	10%
Post-Assessment	Submission of Final Report for the Configuration and Code Review	Within seven (7) calendar days from the completion of training	20%

VIII. MODE OF PROCUREMENT

The mode of procurement shall be Small Value Procurement provided under the Implementing Rules and Regulations (IRR) of Republic Act (R.A.) No. 12009.

IX. INFORMATION SECURITY MANAGEMENT SYSTEM

To ensure the Philippine Competition Commission (PCC) maintains a high standard of information security when engaging with third-party providers, all suppliers are required to comply with the established PCC Information Security Management System (ISMS). These requirements are outlined in the Supplier Security Policy (POL-PCC-GSD 02-03) and related ISMS policies and procedures.

All data, documents, records, configuration files, and metadata (collectively referred to as "Information") provided to the supplier(s) for the purpose of delivering services are considered confidential and remain the exclusive property of the PCC. The supplier(s) shall recognize the critical importance of maintaining the security and confidentiality of the Information and agree to prevent its unauthorized transfer, disclosure, or use by any third party. The supplier(s) shall not use the information for any purpose other than to perform the agreed-upon services. Furthermore, the supplier(s) shall ensure that, upon completion of the service, they will not retain any portion of the Information in any form whatsoever.

The following must be submitted after the issuance of Notice of Award or Purchase Order or Job Order:

- Notarized Non-Disclosure Agreement

The documents will be submitted to the ISMS Secretariat in compliance with the approved PCC Information Security Management System and will not form part of the submission for payment processing.

X. LIQUIDATED DAMAGES

If the supplier fails to deliver any or all of the goods and/or to perform the services within the period specified in the contract, the Procuring Entity shall, without prejudice to its other remedies under this contract and under the applicable law, deduct from the contract price as liquidated damages, the applicable rate of one-tenth (1/10) of one percent (1%) of the cost of the unperformed portion of every day of delay. The maximum deduction shall be ten percent (10%) of the amount of the contract. Once, maximum is reached, the procuring entity reserves the right to rescind the contract, without prejudice to other courses of action and remedies open to it.

XI. DISPUTE AGREEMENT / RESOLUTION

Should any dispute related to the Contract and/or rights of the parties arise, the same shall be submitted to mutual consultation, mediation and arbitration, in the order of application. The venue of the proceedings shall be in Quezon City.

In case of a court suit, the venue shall be the courts of competent jurisdiction in Quezon City, to the exclusion of all other courts; and

Any amendments and additional terms and conditions of the Contract must be in writing, signed and acknowledged by the Parties.

Prepare[confidential]

Signed by Alvin Bosque
ALVIN U. BOSQUE
Information Technology Officer I

Revie[confidential]

Signed by Allan Roy Mordeno
ALLAN ROY D. MORDENO
Chief, ICT Division

Noted by: [confidential]

Signed by Jeson Q de la Torre
JESON Q. DE LA TORRE
Director IV
Administrative Office

RATING CRITERIA FOR BIDDERS

I. Technical Proposal:

CRITERIA	PARAMETERS		RATING SYSTEM
Experience and capability of the firm (20%)	Handled at least three (3) similar contracts. (30%) Note: similar contracts refer to conduct of vulnerability assessment and penetration testing contracts.	100	Submitted more than three (3) certificate of satisfactory service and/or certificate of completion and acceptance
		80	Submitted three (3) certificate of satisfactory service and/or certificate of completion and acceptance
		0	Submitted less than three (3) certificate of satisfactory service and/or certificate of completion and acceptance
	With at least five (5) years of relevant experience on IT security, protection of information assets, risk management and other computer controls. (70%)	100	More than five (5) years
		80	Five (5) years
		0	Less than five (5) years
Applicable years of relevant experience of the firm (10%)	With at least three (3) concluded similar projects	100	More than three concluded similar projects
		80	Three (3) concluded similar projects
		0	Less than three concluded similar projects
Quality of Personnel (20%) Project Lead / Manager	Ten (10) years of relevant experience on IT security, protection of information assets, risk management and other computer controls. (30%)	100	More than ten (10) years
		80	Ten (10) years
		0	Less than ten (10) years
	With at least three (3) relevant certification/s (e.g. ethical hacking,	100	More than three (3) relevant certification submitted

	Security, Cyber Security, Network, Application, etc.) (20%)	80	Three (3) relevant certification submitted
		0	Less than three (3) relevant certification submitted
Team Members	Five (5) years of relevant experience on IT security, protection of information assets, risk management and other computer controls. (30%)	100	More than five (5) years
		80	Five (5) years
		0	Less than five (3) years
	With at least three (3) relevant certification/s (e.g. ethical hacking, Security, Cyber Security, Network, Application, etc.) (20%)	100	More than three (3) relevant certification submitted
		80	Three (3) relevant certification submitted
		0	Less than three (3) relevant certification submitted
Plan of Approach and Methodology (30%)	Timing of Deliverables (40%)	100	**Very Good -** The deliverables are for submission at least two to four days before the required timeline and schedule set by the PCC.
		80	**Good -** The deliverables are for submission on the day of the schedule set by the PCC.
		0	**Poor -** The proposal indicates late submission of the required deliverables.
	Comprehensiveness of the Vulnerability Assessment and Penetration Testing Plan and Methodology (30%)	100	**Very Good –** Provides comprehensive (qualitative and quantitative) report on the results of the vulnerability assessment and penetration testing using an enterprise grade

			tools and manual testing techniques showing extensive severity matrix, threat prioritization and remediation
		80	**Good –** Provides report (qualitative and quantitative) on result using open source and freeware tools and manual testing techniques with limited severity matrix and threat prioritization and remediation
		0	**Poor –** Provides report (qualitative and quantitative) on result using trial software and manual testing techniques with poor severity matrix and threat prioritization and remediation
	Post Assessment and Result of Iterative Vulnerability Assessment and Treatment (VA/T)	100	**Very Good –** Firm's commitment to 100% non-occurrence of identified vulnerabilities in iterative vulnerability assessment
		80	**Good –** Firm's commitment of at most 10% occurrence of identified vulnerabilities in iterative vulnerability assessment.
		0	**Poor –** Firm's commitment of at most 20% occurrence of identified vulnerabilities in iterative vulnerability assessment

II. Financial Proposal (20%)

The Financial Proposals, on the other hand, shall be evaluated based on the following formula:

$$\text{Financial Score} = \frac{LFP}{FP} \text{ X W}$$

Where:

LFP is the amount of the lowest financial proposal.

FP is the amount of the Financial Proposal of the bidder being rated.

W is the weight of the financial proposal, as indicated in the Terms of Reference.

Conforme:

_____

Name and Signature of Authorized Representative

_____

Designation

_____

Name of Company

_____

Date