CREDIT INFORMATION CORPORATION

6F Exchange Corner Building
107 V. A. Rufino Street corner Esteban St.,
Legaspi Village, Makati City 1229
(02) 8236-5900 | www.creditinfo.gov.ph

INVITATION FOR NEGOTIATED PROCUREMENT
Negotiated Procurement – Two Failed Biddings
2022-CIMS(023)-NP2FB-0032c

1. The Credit Information Corporation (CIC), through its Bids and Awards Committee (BAC) invites PhilGEPS registered suppliers to participate in the negotiation for the Vulnerability Assessment and Penetration Testing in accordance with Section 53.1 of the Revised Implementing Rules and Regulations (R-IRR) of Republic Act No. 9184, otherwise known as the "Government Procurement Reform Act".

2. The Approved Budget for the Contract is One Million Five Hundred Thousand Pesos (PhP1,500,000.00) inclusive of all applicable taxes.

3. Interested Bidders may obtain further information from CIC Finance and Administration Group – Procurement Unit at Telephone No. 8236-5900 loc. 134-135 and inspect the Invitation for Negotiated Procurement at the address given below, Tuesdays to Fridays only; from 8:00 AM to 5:00 PM.

4. A complete set of Invitation for Negotiated Procurement may be acquired by the Interested Bidders atExchange Corner Building, 107 V.A. Rufino Street corner Esteban St. Legaspi Village, Makati City, starting September 7, 2022, Tuesdays to Fridays only; from 8:00 AM to5:00 PM, and upon payment of a non-refundable fee amounting to ***PhP5,000.00***. Bidders who have purchased bidding documents during the first and second failed biddings, and the invitation for negotiated procurement during the first negotiated procurement failed bidding, need not pay for the tender documents.

Interested Bidders may also opt to pay through online payment or bank transfer not later than the submission of quotations. Below are the account details:
Credit Information Corporation
Landbank of the Philippines
Current Account No. 1802-1032-27

Bidders shall send the receipt or proof of payment to the Secretariat at the email address provided below, for validation. Once validated, an e-copy of the Official Receipt will be emailed to the Prospective Bidder.

5. The schedule of Procurement Activities of the project is as follows:

Activities	Schedule/Venue
1) Issuance and availability of Invitation for Negotiated Procurement	***Starting September 7, 2022***
2) Negotiation with Prospective Bidders ***Note: The negotiation must be attended by at least one (1) bidder's technical personnel and one (1) official representative***	***September 12, 2022*** (**10:00 AM**) via Zoom Meeting

3) Deadline for the Manual Submission of the Best and Final Offer/Quotations ***Note: Wet signatures are required for quotations***	***September 15, 2022*** (**11:30 AM**) at Credit Information Corporation Lobby, Exchange Corner Building, 107 V.A. Rufino Street corner Esteban St. Legaspi Village, Makati City
4) Opening of Quotations ***Note: Bidders may witness the opening of the quotations via Zoom or in person. One (1) representative per bidder will be allowed entry to the physical venue provided.***	***September 15, 2022*** (**12:00 PM**) at Credit Information Corporation, 4F, Exchange Corner Building, 107 V.A. Rufino Street corner Esteban St. Legaspi Village, Makati City and via Zoom

6. Prospective bidders who are interested in joining the negotiation may contact the BAC Secretariat at the e-mail address provided below to request for a meeting invitation.

7. Prospective bidders are encouraged to write letters of clarification, if any, with regard to the eligibility, technical and financial documents, scope of the project, and terms of reference. **Letters shall be sent to the email address given below. The deadline for the submission of letters is on September 9, 2022 at 4:00 PM.**

8. Interested Bidders shall submit the following documents in a sealed envelope. The envelope label should also contain the name of the bidder, address and contact details of the bidder:

I. ELIGIBILITY DOCUMENTS

1. Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);

II. TECHNICAL DOCUMENTS

1. Original duly signed Omnibus Sworn Statement (OSS).

and if applicable, Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

2. Conformity with the Schedule of Requirements and Technical Specifications

III. FINANCIAL DOCUMENTS

1. Duly accomplished Financial Proposal Forms

9. During post-qualification, the following shall be required:

a. Income Tax Returns for taxable 2021 (BIR Form 1701 or 1702); and

b. Value Added Tax Returns (Forms 2550M and 2550Q) or Percentage Tax Returns (Form 2551M) covering the six months immediately prior to the opening of bids.

Only tax returns filed and taxes paid through the Electronic Filing and PaymentSystem (EFPS) shall be accepted.

10. The CIC reserves the right to accept or reject any bid/proposal, annul the bidding process, and to reject all bids/proposals at any time prior to contract award, without thereby incurring any liability to the affected bidder/s.

11. For further information, please refer to:

BAC Secretariat
Credit Information Corporation
4F Exchange Corner Building
107 V.A. Rufino cor. Esteban & Bolanos Sts.
Legaspi Village, Makati City
Telephone Nos. (632) 8236-5900 loc. 134-135
Email address: procurementunit@creditinfo.gov.ph

SIGNED
MARIA LOURDES L. RIFAREAL
BAC Chairperson

Annex "A"

Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

Lot	Description	Delivery Schedule
1	Vulnerability Assessment and Penetration Testing	Within fifteen (15) calendar days upon receipt of the Notice to Proceed

Contract Duration: CIC shall engage the services of the Service Provider for an estimated period of forty-five (45) calendar days, excluding remediation period of the CIC.

_____	_____	_____
Name of Company	Signature over Printed Name of Authorized Representative	Date

Annex "B"

Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.

Terms of Reference

1. Overview

The Credit Information Corporation (CIC) is a Government-Owned and Controlled Corporation (GOCC) created in 2008 by virtue of Republic Act No. 9510 otherwise known as the Credit Information System Act (CISA). The CIC is mandated to establish a comprehensive and centralized Credit Information System (CIS) for the collection and dissemination of fair and accurate information relevant to, or arising from credit and credit-related activities of all entities participating in the financial system, such as but not limited to retail, trade, utilities, and other service and product providers that may yield data on creditworthiness and payment behavior.

2. Purpose

The CIC anticipates conducting an information security review of the underpinning application systems of the Credit Information System (CIS), and a social engineering attack simulation to cover CIC employees. Due to the technical nature of the project and requirements, the CIC is seeking the assistance of an external Security Service Provider to perform a Vulnerability Assessment and Penetration Testing (VAPT) activity to help the CIC achieve the following:

- Gain a better understanding of potential vulnerabilities and threats that may be visible from an external network;
- Assess and identify all weaknesses in the CIS application and other web applications of the CIC;
- Identify the risk level where CIC is exposed to so that appropriate countermeasures can be developed and applied;
- Raise awareness on Cybersecurity threats by conducting a social engineering attack simulation to CIC employees; and
- Provide the CIC a platform for its continual security awareness and training campaign.

The Service Provider shall undertake all necessary steps, employ suitable strategies, and make available appropriately equipped personnel in all phases of the engagement.

3. Scope

The scope of the penetration test of this engagement will be limited to the external-facing network services and resources of the CIC. Likewise, the scope of the vulnerability assessment will be limited to CIC's production environment underpinning the CIS (see. Below for details). The project shall also include social engineering simulation on its management and employees.

The security review will consist of a black-box and grey-box technical assessment, and one-time social engineering simulation exercises deemed relevant by the Service Provider. The black box approach is a limited knowledge security assessment that simulates a real-life attack against the application from unauthorized users. The grey box approach is a follow-up assessment to the earlier approach. Detailed information about the target applications will be provided to the Service Provider, such as IP addresses, operating system details, server function, and a user account to the

application;

Below is a list of CIC external hosts that will be considered for the external security review:

- Four (4) websites
- One (1) SFTP service
- One (1) FTPS service
- Two (2) application programming interface gateways

Below is a list of CIC internal hosts that will be considered for the vulnerability assessment (some are back-end of the resources subject for external assessments):

- Eleven (11) Application Servers running Windows Server and IIS
- Four (4) Database Servers running Enterprise Linux Server
- Eleven (11) Support Apps running Windows Server
- Two (2) Support Apps running Enterprise Linux Server

Finally, the social engineering simulation component will cover CIC employees, management, and members of the Board of Directors.

4. Responsibilities of the CIC

CIC's responsibilities with respect to this project are as follows:

1. Grant the Service Provider's authorized representative access to its premises, equipment and facilities located therein to perform its obligations, provided that such representative shall be accompanied by the duly assigned personnel of the CIC Technical Support Department.

2. Secure the necessary access pass and building permit required by the facility administrator and assume responsibility for the safe custody and use of the equipment installed by the Service Provider.

3. Monitor the provided services and verify if the parameters under the Service Level Agreement are met and performed by the Service Provider.

4. Issuance of a Certificate of Inspection and Acceptance to the Service Provider upon successful completion of the testing certifying that the Service Provider conforms to all requirements stipulated in this document.

5. Pursuant to General Procurement Policy Board (GPPB) Resolution No. 019-2006 dated 06 December 2006, at the end of each year, the CIC will conduct an assessment of the quality of service provided particularly the cost charged by the Service Provider and the range of services it offers against other service providers in the area.

5. Requirements

5.1. General

Items	Requirements	Statement of compliance ("Comply' or "Not Comply")	Evidence of Compliance
1. Service Provider	a) The Service Provider has been in the business of providing VAPT services for private and/or government financial institutions, for at least five (5) years prior to the deadline for the submission of bids. (Provide reference of Government clients). b) The Service Provider must establish a single point of contact helpdesk with hotline numbers to provide timely and responsive trouble reporting, incident handling, problem escalation and field support for all problem related issues. c) The Service Provider is a recognized Cybersecurity Assessment Provider by the DICT. d) If access to CIC premises will be needed, the Service Provider must abide by the rules stated in MACEA Advisory 2020-0826: "Workplace Prevention and Control of COVID-19," as well as building requirements on negative COVID-19 tests.		
2. Service Delivery Manager	a) The Service Provider should assign a Service Delivery Manager (SDM) to CIC for the project to ensure all requirements of this contract are successfully delivered to CIC. b) The SDM should have at least three (3) year service delivery or project management experience in handling similar project implementation. (Provide curriculum vitae and related certifications) c) Minimum five (5) years of		

	experience in managing IT projects, and three (3) years of managing information security audits; d) Relevant experience in managing projects related to Bangko Sentral ng Pilipinas (BSP) Circular 982 – Enhanced Guidelines on Information Security Management		
3. Technology Specialists	a) The Service Provider should assign a Technology Specialist/Engineer to the project. They must be permanent employees of the Service Provider for at least one (1) year. (Provide Certificate of Employment, updated curriculum vitae & related certifications). b) Has at least three (3) year experience in information security review or audit especially in conducting network and application layer penetration testing; c) Has active penetration testing certification from globally recognized certification providers such as the US DoD recognized IA Workforce Certification Providers. (https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/)		

Please refer to **Appendix A** for the **Evaluation Score Sheet.**

5.2. Required Activities

The activity will be performed in two (2) passes after the project kick-off, followed by the social engineering simulation activity.

Items	**Requirements**
First Pass	
Reconnaissance	Discover and identify information from the Internet and other available resources (Dark Web, OSINT, etc.), all information that will represent CIC's Internet footprint. Report the information gathered as well as the methodology on how the information was discovered.

Identity Vulnerabilities	Probe resources (discovered/in-scope) to identify listening services. Identify and assess vulnerabilities that may be present in those exposed services. Produce a prioritized list of security vulnerabilities.
Exploit	Attempt to exploit identified vulnerabilities using a combination of automated and manual tests to uncover all potential issues and may not be limited to the following Open Web Application Security Project (OWASP) top 10 application security risks: 1. All forms of Injection flaws; 2. Cross-Site Scripting (XSS) which may allow attackers to execute scripts in the victim's browser to hijack user sessions; 3. Security misconfiguration of the systems involved; 4. Missing Function Level Access Control which may let attackers to forge application requests in order to access functionality in CIC web applications without proper authorization; 5. Using Components with Known Vulnerabilities which may undermine CIC's application defenses, and enable a range of possible attacks. 6. Broken Authentication and Session Management which may allow attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws. 7. Insecure Direct Object References which may allow attackers to manipulate insecurely exposed references to an internal implementation object to access sensitive data. 8. Sensitive Data Exposure which may allow attackers to steal or modify weakly protected sensitive data to conduct fraud, identity theft, or other crimes. 9. Cross-Site Request Forgery (CSRF) which may allow attackers to force the victim's browser to generate requests. 10. Invalidated Redirects and Forwards which may allow attackers to redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.
Review of Application Architecture.	Attempt to find, download, and review server-side scripts, configuration files, include files and HTML source codes. Check for issues such as database connection strings, configuration settings, unauthorized directory listings and commented code.
Analyze Risk	Evaluate the identified areas of weakness, and rate the findings based on the risk that each poses to CIC assets. **The SP shall use CIC's risk rating criteria as described in Annex C.**

Second Pass/Validation	
	The Service Provider will perform a second pass to validate the implementation of the recommendations during the first pass. The activity will be performed after CIC has implemented the recommended measures to mitigate identified risks. Please refer to the project timeline below. The Service Provider shall perform similar procedures as described above to validate if findings in the First Pass has been resolved.
Social Engineering Simulation	
Phishing and other social engineering simulation activities	1. Secure clearance from the CIC prior to start of the engagement for the conduct of pre-assessment, noting the relevant policies and the existing training of the CIC employees. 2. Perform information gathering and develop the simulation plan of activities with CIC. 3. Based on the agreed terms of procedures and conditions, coordinate with the relevant parties for the conduct of the Phishing and other social engineering attack simulation activities; 4. Based on the result of the Phishing and other social engineering attack simulation activities, assess the awareness of CIC employees, and communicate the same with the CIC management.

5.3. Deliverables

The Service Provider shall submit and present to CIC, based on the scope of work, and in accordance with the timeline, a comprehensive report consisted the following:

Items	**Requirements**
Project Plan	Submission of a project plan detailing all the dates for the work phase, deliverables, review meetings, report delivery and report allocations.
Interim Report	Submission of an interim report in the form of threat and vulnerability matrix that details the description of the vulnerabilities, impact and criticality of the vulnerabilities, impact and criticality and recommendation.
Executive Report	Submission of an executive summary report detailing the engagement's scope, approach and summary recommendations aimed at senior management. Must contain non-technical description of all findings along with discussions of the inherent business risks and recommended risk management strategies.

Technical Report	Submission of a technical report covering identified security risks, exposures and proposed recommendation aimed at technical staff and should provide them with complete solutions.
Executive presentation.	A presentation of the identified risks during the first and second pass to the IT & Cyber Security Committee of the board of directors.
Phishing simulation report	Submission of a phishing simulation activity report covering identified risks pertaining to employee security awareness.

6. *Project Timeline*

CIC shall engage the services of the Service Provider for an estimated period of forty-five (45) calendar days, excluding remediation period of the CIC. The examination of the systems shall be undertaken during off-office hours and subject to reasonable guidelines of the CIC. Any amendment/modification of the work schedules shall be made only upon prior written approval of the CIC Technical Working group, in which case, the engagement shall be correspondingly extended for such period called for by the amendment/modification under the same terms, with no additional cost on the part of CIC.

Below is the proposed timeline of the project:

Activities	**W1**	**W2**	**W3**	**W4**	**W5**	**W6-114**	**W15**	**W16**
First pass								
Validation meeting								
Interim report								
Social engineering simulation & report								
Presentation to the IT & Cyber Security Committee 1								
Remediation by CIC								
Second pass								
Validation meeting								
Submission of final reports								
Presentation to the IT & Cyber Security Committee 2								

ANNEX C: Information Security Risk Assessment Criteria

When assessing the severity of each risk, the assessor must use the following rating criteria to align the activity with CIC's enterprise risk management requirements. The severity of the risk is the sum of the risk's impact value and likelihood rating value. These are discussed in the following tables:

Impact Rating	**Severe**	**5**	• The risk may result in a major loss to confidentiality, integrity, and availability of information and information systems; • The in-scope system is hosting business-critical application and database;
	Major	**4**	• The risk may result in a major loss to confidentiality, integrity, and availability of information and information systems; • The in-scope system is hosting support applications;
	Moderate	**3**	• The risk may result in a considerable loss to confidentiality, integrity, and availability of information and information systems; • The in-scope system is hosting network services;
	Minor	**2**	• The risk may result in a minor loss to confidentiality, integrity, and availability of information and information systems; • The in-scope system is hosting non-critical services;
	Minimal	**1**	• The risk may cause no loss to confidentiality, integrity, and availability of information and information systems; • The in-scope system is hosting non-critical services;
Likelihood Rating	**Almost Certain**	**5**	• Threat source (adversary) is highly-motivated and sufficiently capable; and • The CIC has no security controls in place to prevent the vulnerability from being exercised;
	Likely	**4**	• Threat source (adversary) is highly-motivated and capable; and • The CIC has security controls in place but are less effective to prevent the vulnerability from being exercised;
	Possible	**3**	• Threat source (adversary) is motivated and capable; and • The CIC has security controls in place that may prevent the vulnerability from being exercised;
	Unlikely	**2**	• Threat source (adversary) is motivated but lacks capability; and • The CIC has security control in place that can effectively prevent the vulnerability from being exercised;
	Rare	**1**	• Threat source (adversary) lacks motivation and capability; and • The CIC has two or more security controls in place (layered defense) that can effectively prevent the vulnerability from being exercised;

Risk Rating = Likelihood + Impact

Low = 2-3; Moderate = 4-6; High = 7-8; Extreme = 9-10

Likelihood/ Impact	*Rare (1)*	*Unlikely (2)*	*Possible (3)*	*Likely (4)*	*Almost Certain (5)*
Critical (5)	Moderate 6	High 7	High 8	Extreme 9	Extreme 10
Major (4)	Moderate 5	Moderate 6	High 7	High 8	Extreme 9
Moderate (3)	Moderate 4	Moderate 5	Moderate 6	High 7	High 8
Minor (2)	Low 3	Moderate 4	Moderate 5	Moderate 6	High 7
Insignificant (1)	Low 2	Low 3	Moderate 4	Moderate 5	Moderate 6

The Service Provider must submit a **Description of the Methodology and Work Plan for Performing the Project using "Annex G"** during the submission of price quotation.

The winning bidder of the previous Vulnerability Assessment and Penetration Testing (VAPT) is not eligible to participate in this year's bidding in order to acquire a new set of VAPT testers that will provide a new set of external views, new skill sets and bring in fresh perspectives from the previous Service Provider. However, they still can participate in next year's bidding.

_____	_____	_____
Name of Company	Signature over Printed Name of Authorized Representative	Date

Annex "D"

Omnibus Sworn Statement (Revised)

[shall be submitted with the Bid]

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF_____) S.S.

AFFIDAVIT

I, [Name of Affiant], of legal age, [Civil Status], [Nationality], and residing at [Address of Affiant], after having been duly sworn in accordance with law, do hereby depose and state that:

1. *[Select one, delete the other:]*

   [If a sole proprietorship:] I am the sole proprietor or authorized representative of [Name of Bidder] with office address at [address of Bidder];

   [If a partnership, corporation, cooperative, or joint venture:] I am the duly authorized and designated representative of [Name of Bidder] with office address at [address of Bidder];

2. *[Select one, delete the other:]*

   [If a sole proprietorship:] As the owner and sole proprietor, or authorized representative of [Name of Bidder], I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney;

   [If a partnership, corporation, cooperative, or joint venture:] I am granted full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for [Name of the Project] of the [Name of the Procuring Entity], as shown in the attached [state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)];

3. [Name of Bidder] is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board, by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines onBlacklisting;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. [Name of Bidder] is authorizing the Head of the Procuring Entity or its duly authorized

representative(s) to verify all the documents submitted;

6. *[Select one, delete the rest:]*

   [If a sole proprietorship:] The owner or sole proprietor is not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a partnership or cooperative:] None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   [If a corporation or joint venture:] None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards; and

8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   a. Carefully examining all of the Bidding Documents;
   b. Acknowledging all conditions, local or otherwise, affecting the implementation of the Contract;
   c. Making an estimate of the facilities available and needed for the contract to be bid, if any; and
   d. Inquiring or securing Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity.

10. *In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government ofthe Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.*

IN WITNESS WHEREOF, I have hereunto set my hand this___day of____, 20__at _____, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

SUBSCRIBED AND SWORN to before me this day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M.No. 02-8-13-SC). Affiant/s exhibited to me his/her [insert type of government identification card used], with his/her photograph and signature appearing thereon, with no._____ and his/her Community Tax Certificate No._____ issued on_____ at_____.

Witness my hand and seal this____ day of *[month] [year]*.

NAME OF NOTARY PUBLIC
Serial No. of Commission _____
Notary Public for_____ until_____
Roll of Attorneys No._____
PTR No._____ *[date issued], [place issued]*
IBP No._____ *[date issued], [place issued]*

Doc. No. Page No. Book No. Series of _____

Annex "E"

Financial Proposal Form

[Date]

Ms. MARIA LOURDES L. RIFAREAL
Chairperson
Bids and Awards Committee

Dear Ms. Rifareal:

The undersigned offer to provide the services for [Title of Project] in accordance with your Negotiation Documents dated [insert date] and our Legal/Technical Requirements. Our attached Financial Proposal is for the sum of [amount(s) in words and figures].

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the bid validity period of one hundred twenty (120) calendar days from the date of the opening of proposals/offers.

We confirm that we have read, understood and accept the contents of the Negotiation Documents, Terms of Reference (TOR), the provisions relating to the eligibility of Supplier and the applicable guidelines for the procurement rules of the government of the Philippines, and other attachments and inclusions included in the Negotiation Documents sent to us.

We understand you are not bound to accept any offer you receive.

Sincerely yours,

[Signature]
[Name of Authorized Signatory]
[Name of Firm]
[Address]

Annex "F"

Financial Proposal

Negotiated Procurement – Two Failed Biddings
Vulnerability Assessment and Penetration Testing
2022-CIMS(023)-NP2FB-0032c

NO.	*DESCRIPTION*	*QTY*	*UNIT*	*UNIT COST (PHP)*	*TOTAL COST ABC (PHP)*	*BIDDER'S OFFER*	
						UNIT COST (PHP)	*TOTAL COST (PHP)*
1	***Vulnerability Assessment and Penetration Testing***	1	lot	1,500,000.00	1,500,000.00		
			TOTAL BID AMOUNT				

NAME OF COMPANY

ADDRESS

SIGNATURE OVER PRINTED NAME

CONTACT NO.

Annex "G"

DESCRIPTION OF THE METHODOLOGY AND WORKPLAN FOR PERFORMING THE PROJECT

APPENDIX A

The overall passing rate is eighty percent (80%).

Evaluation Score Sheet		
CRITERIA	**WEIGHT**	**SCORE**
A. TECHNICAL	100.00%	100.00%
A.1. Relevant Experience of the Service Provider	20.00%	20.00%
Number of successfully completed contracts analogous to VAPT services in private and/or government financial institutions within the last 5 years	20.00%	
5 and more contracts	20.00%	
3-4 contracts	15.00%	
1-2 Contracts	10.00%	
No contracts	0.00%	
A.2. Relevant Education and Experience of Key Personnel	55.00%	55.00%
A.2.1. Service Delivery Manager	10.00%	
A.2.1.1. Education	5.00%	
Bachelor's Degree, related field with Project Management Certification such as PMP or Prince2, and ITSM: ITIL Foundation	5.00%	
Bachelor's Degree, non-related with Project Management Certification such as PMP or Prince2, and ITSM: ITIL Foundation	4.00%	
Bachelor's Degree, related field	3.00%	
Bachelor's Degree, non-related field	2.00%	
Non-Bachelor's Degree	0.00%	
A.2.1.2. Experience	5.00%	
A.2.1.2.1. The SDM should have at least three (3) year service delivery or project management experience in handling similar project implementation.	1.00%	
3 years or more experience;	1.00%	
Less than 3 year experience;	0.00%	
A.2.1.2.2. Minimum five (5) years of experience in managing IT projects, and three (3) years of managing information security audits;	2.00%	
Has the minimum required experience;	2.00%	
Less than the minimum required experience;	0.00%	
A.2.1.2.3. Relevant experience in managing projects related to Bangko Sentral ng Pilipinas (BSP) Circular 982- Enhanced Guidelines on Information Security Management	2.00%	
Has the required relevant experience;	2.00%	
Does not have the required relevant experience;	0.00%	

A.2.2. Technology Specialists	45.00%	
A.2.2.1. Education	5.00%	
Bachelor's Degree, related field	5.00%	
Bachelor's Degree, non-related field	3.00%	
Non-Bachelor's Degree	0.00%	
A.2.2.2. Experience and Related Training	40.00%	
A.2.2.2.1. Must be permanent employees of the Service Provider	5.00%	
1 year or more work experience with Service Provider;	5.00%	
Less than 1 year work experience;	0.00%	
A.2.2.2.2. Has at least three (3) year experience in information security review or audit especially in conducting network and application layer penetration testing;	5.00%	
Has the minimum required experience;	5.00%	
Less than the minimum required experience;	0.00%	
A.2.2.2.3. Has active penetration testing certification from globally recognized certification providers (US DoD recognized IA Workforce Certification Providers).	30.00%	
Has any of the minimum certifications from globally recognized certification providers (US DoD recognized IA Workforce Certification Providers) and advanced Penetration Testing certification such as GPEN, OSCP and LPT.	30.00%	
Has any of the minimum certifications from globally recognized certification providers (US DoD recognized IA Workforce Certification Providers).	15.00%	
Does not have any of the required certification;	0.00%	
A.3. Strict Adherence to the Terms of Reference, or similar Approach and Methodology	25.00%	25.00%
Substance	15.00%	
Completeness	5.00%	
Clarity	5.00%	
TOTAL	**100.00%**	**100.00%**