



**May 28, 2021**

**REQUEST FOR PROPOSAL**  
**No.: 2021-CIMS(025)-NPSVP-022**

**Vulnerability Assessment and Penetration Testing**  
**(Negotiated Procurement – Small Value Procurement)**

Sir/Madam:

The Credit Information Corporation invites you to submit proposal for the item/s described below subject to the Instructions (**Annex "A"**) and Terms of Reference (**Annex "B"**).

Qty	UOM	PARTICULARS	Unit Cost	Approved Budget for the Contract
1	lot	Vulnerability Assessment and Penetration Testing	<b>PhP900,000.00</b>	<b>PhP900,000.00</b>

Contract Duration: One (1) Year  
 Delivery Schedule: Thirty (30) calendar days upon receipt of Notice to Proceed  
 Delivery Site: 6F, Exchange Corner Bldg., 107 VA Rufino St. cor. Esteban St., Legaspi Village, Makati City

Only one (1) set of documents, certified to be true copies of the original, shall be required. See detailed Instructions (**Annex "A"**).

Proposals and other documents required may be sent electronically to [phoebe.wagan@creditinfo.gov.ph](mailto:phoebe.wagan@creditinfo.gov.ph). Electronically submitted proposals and documents must be submitted on or before the deadline of submission as stated in this RFQ.

The CIC reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract consistent with Section 41 of the IRR of RA 9184.

**Signed**  
**PHOEBE ANN R. WAGAN**  
Administrative Services Officer V

## INSTRUCTIONS

1. This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the Provisions of RA 9184 and its IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation.
2. The applicable rules and regulations for the procurement of consulting services under RA 9184 will govern this Contract.
3. The Quality- Cost Based Evaluation procedure will be used to evaluate the proposals. The criteria and corresponding weights are allocated as follows:

Technical Proposal		85%
Relevant Experience of the Service Provider	20%	
Relevant Education and Experience of Key Personnel	40%	
Strict Adherence with TOR/ Approach and Methodology	25%	
Financial Proposal		15%
Total Score		100%

Note: Please see **Annex "K"** (QCBE Parameters) for details.

4. The over-all passing rate is seventy (70).

The minimum technical score to pass is seventy (70). A Zero (0) score from any of the subcriteria set in Annex "K" shall automatically obtain a total technical score of Zero (0). Only the financial proposals of consultants who meet the minimum technical score of 70 shall be opened. The TWG will open and evaluate the financial proposals immediately after the determination of the technical bids which passed the minimum technical score.

5. Only one (1) set of documents, duly certified as true copies of original, shall be required. The set shall be comprised as follows:

### 5.1. First Envelope

#### 5.1.1. Eligibility Documents

- 5.1.1.1. Mayor's/ Business Permit for the current year;
- 5.1.1.2. PhilGEPS Registration Number;
- 5.1.1.3. Latest Income/ Business Tax Return;
- 5.1.1.4. Omnibus Sworn Statement (Annex C), duly supported with authority of the signatory which may be either a Special Power of Attorney (for sole proprietorship) or a Board Secretary's Certificate (for partnerships or corporations);

#### 5.1.2. Technical Documents

- 5.1.2.1. TPF<sup>1</sup> 1. Technical Proposal Submission Form;
- 5.1.2.2. TPF 2. Relevant Services Carried out in the Last Five Years That Best Illustrate Qualifications (One TPF 2 Form must be accomplished for each Contract/ project previously carried out);
- 5.1.2.3. TPF 3. Description of Methodology/ TPF 6. Workplan for Performing the Project;
- 5.1.2.4. TPF 4. Team Composition and Tasks;

---

<sup>1</sup> Technical Proposal Form

5.1.2.5. TPF 5. Format of Curriculum Vitae (CV) for Proposed Personnel (For each Key Personnel).

5.2. Second Envelope

5.2.1. Financial Documents

5.2.1.1. FPF<sup>2</sup> 1. Financial Proposal Submission Form;

5.2.1.2. FPF 2. Summary of Costs

6. In the interest of time, the following supporting documents may be submitted, if not yet currently available, anytime: (a) during submission of proposals, (b) evaluation of proposals, or (c) after issuance of the Notice of Award, but before payment.

6.1. PhilGEPS Registration Number; and/ or

6.2. Mayor's/ Business Permit for the Year 2021.

PhilGEPS Platinum Registration Certificate may be submitted in lieu of the foregoing documents. The Omnibus Sworn Statement may be submitted unnotarized subject to compliance therewith after award of contract but before payment.

7. For manual submission, the address for the submission of proposals is **GF, Exchange Corner Bldg., 107 VA Rufino St. cor. Esteban St., Legaspi Village, Makati City.**

Activity	Date	Time
Manual Submission of Proposals	June 1, 2021 (Tuesday) and June 3, 2021 (Thursday)	9:00 AM – 3:00 PM
Electronic Submission of Proposals	May 28, 2021 – June 4, 2021	8:00 AM – 5:00 PM
Deadline for Submission and Opening of Proposals	June 4, 2021	5:00 P.M.

8. In case consultants opt to submit their proposals electronically, the contents of the first envelope and the second envelope may be separately packaged and secured using symmetric encryption or stored in an archive or zip file protected with a password before emailing them to [phoebe.wagan@creditinfo.gov.ph](mailto:phoebe.wagan@creditinfo.gov.ph). Passwords to the zipped file shall be shared to the CIC- through SMS, email, facsimile, telephone call, or any other forms of electronic messaging, during the scheduled bid opening date and time.

9. The address for the opening of proposals is **4F, Exchange Corner Bldg., 107 VA Rufino St. cor. Esteban St., Legaspi Village, Makati City.** The date and time for the opening of proposals is **June 4, 2021; 5:00 PM.**

10. The following processes for the opening and evaluation of bids shall be adopted:

10.1. The technical proposal together with the financial proposal shall be considered in the ranking of consultants. The technical proposals shall be evaluated first using the criteria described in Instruction No. 3. The financial proposals of the consultants who meet the minimum technical score shall then be opened.

10.2. The financial and technical proposals are given corresponding weights of fifteen percent (15%) and eighty five percent (85%), respectively. The CIC-BAC through the Administration Unit shall rank the consultants in descending order based on the combined numerical ratings of their technical and financial proposals and identify the Highest Rated Bid.

---

<sup>2</sup> Financial proposal Form

10.3. The CIC-BAC through the Administration Unit shall recommend to the HoPE the award of contract in favor of consultant with the Single or Highest Rated and Responsive Proposal. In case of approval, the HoPE shall immediately enter into contract with the said consultant.

11. The financial evaluation shall include all such taxes, duties, fees, levies, and other charges imposed under applicable laws.

12. The financial proposals shall be rated as follows:

The lowest Financial Proposal (FI) shall be given a Financial Score (Sf) of 100 points. The Sf of other Financial Proposals shall be computed based on the formula indicated below:

$$Sf = 100 \times FI/F$$

Where:

Sf is the financial score of the Financial Proposal under consideration,

FI is the lowest Financial Proposal, and

F is the Financial Proposal under consideration.

13. Using the formula  $S = St \times T\% + Sf \times F\%$ , the Bids shall then be ranked according to their combined St and Sf using the weights (St is the technical score of the Technical Proposal under consideration; T = the weight given to the Technical Proposal; F = the weight given to the Financial Proposal;  $T + F = 1$ ) indicated below:

T \_\_\_\_\_ (85%); and

F \_\_\_\_\_ (15%);

provided that the total weights given to the Technical and Financial Proposals shall add up to 1.0.

## **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 for 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 this engagement will be limited to external facing network services and resources. Likewise, the project shall also include social engineering simulation on its management and employees. The security review will consist of black-box and grey-box technical assessment, and one-time phishing and other social engineering simulation exercise 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 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 security review:

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

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**

<b>Items</b>	<b>Requirements</b>
1. Service Provider	a) The Service Provider has been in business of providing VAPT services for financial and government institutions, for

	<p>at least five (5) years prior to the deadline for the submission of bids. (Provide reference of Government clients)</p> <p>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.</p> <p>c) The Service Provider is a recognized Cybersecurity Assessment Provider by the DICT.</p> <p>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.</p>
2. Service Delivery Manager	<p>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.</p> <p>b) The SDM should have at least three (3) year service delivery of project management experience in handling similar project implementation. (Provide curriculum vitae and related certifications)</p> <p>c) Minimum five (5) years of experience in managing IT projects, and three (3) years of managing information security audits;</p> <p>d) Relevant experience in managing projects related to Bangko Sentral ng Pilipinas (BSP) Circular 982 – Enhance Guidelines on Information Security Management</p>
3. Technology Specialists	<p>a) The Service Provider should assign at least two (2) Technology Specialists/Engineers 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 &amp; related certifications).</p> <p>b) Has as least three (3) years experience in information security review or audit especially in conducting network and application layer penetration testing;</p> <p>c) Has active certification of at least one of the following GPEN, LPT or OCPC;</p>

## 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
<b>First Pass</b>	
<i>Reconnaissance</i>	<p>Discover and identify information from the Internet and other available resources (Dark Web, OSINT, etc.), all information that will represent CIC's Internet footprint.</p> <p>Report the information gathered as well as the methodology on how the information was discovered.</p>
<i>Identity Vulnerabilities</i>	<p>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.</p>
<i>Exploit</i>	<p>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:</p> <ol style="list-style-type: none"> <li>1. All forms of Injection flaws;</li> <li>2. Cross-Site Scripting (XSS) which may allow attackers to execute scripts in the victim's browser to hijack user sessions;</li> <li>3. Security misconfiguration of the systems involved;</li> <li>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;</li> <li>5. Using Components with Known Vulnerabilities which may undermine CIC's application defenses, and enable a range of possible attacks.</li> <li>6. Broken Authentication and Session Management which may allow attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws.</li> <li>7. Insecure Direct Object References which may allow attackers to manipulate insecurely exposed references to an internal implementation object to access sensitive data.</li> </ol>



	<ol style="list-style-type: none"> <li>8. Sensitive Data Exposure which may allow attackers to steal or modify weakly protected sensitive data to conduct fraud, identity theft, or other crimes.</li> <li>9. Cross-Site Request Forgery (CSRF) which may allow attackers to force the victim's browser to generate requests.</li> <li>10. Invalidated Redirects and Forwards which may allow attackers to redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.</li> </ol>
<i>Review of Application Architecture.</i>	Attempt to find, download, and review server-side scripts, configuration files, include files and the HTML source codes. Check for issues such as database connection strings, configuration settings, unauthorized directory listings and commented code.
<i>Analyze Risk</i>	Evaluate the identified areas of weakness, and rate the findings based on the risk that each poses to the CIC. The SP shall use CIC's risk rating criteria as described in Annex A.
<b>Second Pass/Validation</b>	
	<p>The Service Provider will perform a second pass to validate the implementation of the recommendations during the first pass.</p> <p>The activity will be performed after the CIC has implemented the recommended measure to mitigate identified risks. Please refer to the project timeline below.</p> <p>The Service Provider shall perform similar procedures as described above to validate if findings in the First Pass have been resolved.</p>
<b>Social Engineering Simulation</b>	
Phishing and other social engineering simulation activities	<ol style="list-style-type: none"> <li>1. Secure clearance from the CIC to start of the engagement for the conduct of pre-assessment, noting the relevant policies and existing training of the CIC employees.</li> <li>2. Perform information gathering and develop the simulation plan of activities with CIC.</li> <li>3. Based on the agreed terms of procedures and conditions, coordinates with the relevant parties for the conduct of the Phishing and other social engineering attack simulation activities;</li> <li>4. Bases on the result of the Phishing and other social engineering attack simulation activities, assess the</li> </ol>

	awareness of the CIC employees, and communicate the same with CIC management.
Attack simulation and e-learning platform	<ol style="list-style-type: none"> <li>1. Provide a phishing and e-learning platform that is listed as leader in Gartner Magic Quadrant for Security Awareness Computer-Based Training for <b>seventy-five users (75)</b>;</li> <li>2. The platform will be used to perform basic attack simulations and provide followup e-learning content, to enable the CIC to continue its campaign after the end of the engagement.</li> <li>3. The platform must support the following: <ol style="list-style-type: none"> <li>a. Phishing simulator <ul style="list-style-type: none"> <li>▪ Built-in phishing templates</li> <li>▪ Easy to use template builder</li> <li>▪ Phished learner training</li> </ul> </li> <li>b. Security awareness training <ul style="list-style-type: none"> <li>▪ Provide training modules, videos</li> <li>▪ Pre-built training plans</li> <li>▪ Personalized &amp; role-based training</li> <li>▪ Industry &amp; compliance training</li> <li>▪ Posters, newsletters &amp; supporting resources</li> </ul> </li> <li>c. Learning experience <ul style="list-style-type: none"> <li>▪ Personalized learner dashboard</li> <li>▪ Gamified &amp; experiential learning</li> <li>▪ Training recommendations</li> <li>▪ Course completion certificates</li> </ul> </li> <li>d. Reporting &amp; assessments <ul style="list-style-type: none"> <li>▪ Dashboard reports</li> <li>▪ Learner activity &amp; risk scores</li> <li>▪ Automated campaign reports</li> <li>▪ Assessments</li> <li>▪ Industry benchmarks</li> </ul> </li> </ol> </li> </ol>

### 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 sixty (60) 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	W7-16	W17	W18
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										

### 7. Schedule of Delivery

The Service Provider shall commence delivery and implementation of the services within 30 calendar days upon receipt of the Notice to Proceed.

### 8. Terms of Payment

Payment shall be made on the following:

1. The total contract cost which shall be paid in full after completion of the project subject to the acceptance of the deliverables by the Inspection and Acceptance Committee.
2. Payment shall be made based on the schedule below and subject to submission of billing statement, and other supporting documents by the Service Provider.

1.	Upon completion of the interim report & social engineering report	90%
2.	Upon submission of the Final Report	10%
	Total	100%

## **Omnibus Sworn Statement**

---

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 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 of *[Name of Bidder]*, I have full power and authority to do, execute and perform any and all acts necessary to represent it in the bidding for *[Name of the Project]* of the *[Name of the Procuring Entity]*;

*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 and/or to represent the *[Name of Bidder]* in the bidding as shown in the attached *[state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate issued by the corporation or the members of the joint venture)]*;

**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;**

**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:* I am 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;

8. *[Name of Bidder]* is aware of and has undertaken the following responsibilities as a Bidder:

a) Carefully examine all of the Bidding Documents;

b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

c) Made an estimate of the facilities available and needed for the contract to be bid, if any; and

d) Inquire or secure 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; and

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 of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

11. *[Name of Bidder]* hereby assigns the following contact number/s and e-mail address/es as the official telephone/fax number and contact reference of the company where the CIC BAC and CIC notices may be transmitted.

Telephone No/s.: \_\_\_\_\_  
Fax No/s.: \_\_\_\_\_  
E-mail Add/s.: \_\_\_\_\_

It is understood that notices/s transmitted in the above-stated telephone/fax numbers and/or e-mail address/es are deemed received as of its transmittal and the reckoning period for the reglementary periods stated in the bidding documents and the revised Implementing Rules and Regulations of Republic Act No. 9184 shall commence from receipt thereof.

IN WITNESS WHEREOF, I have hereunto set my hand this \_\_\_ day of \_\_\_\_\_, 2017 at \_\_\_\_\_, Philippines.

\_\_\_\_\_  
Bidder's Representative/Authorized  
Signatory

**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. \_\_\_\_\_ .

Witness my hand and seal this \_\_\_ day of *[month]* *[year]*.

**NAME OF NOTARY PUBLIC**

Doc. No. \_\_\_\_  
Page No. \_\_\_\_  
Book No. \_\_\_\_  
Series of \_\_\_\_.

Note:

*"Sec. 12. Competent Evidence of Identity – The phrase "competent evidence of identity" refers to the identification of an individual based on:*

At least one current identification document issued by an official agency bearing the photograph and signature of the individual, such as but not limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, Philhealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification;

The Board Resolution or Secretary's Certificate referring to the said Board Resolution designating the bidder's authorized representative and signatory need not specifically indicate the particular project where such authority is given provided that the said authority covers activities by CIC.



**TPF 1. TECHNICAL PROPOSAL SUBMISSION FORM**

*[Date]*

*[Name and address of the Procuring Entity]*

Ladies/Gentlemen:

We, the undersigned, offer to provide the consulting services for [ *Title of Project*] in accordance with your Request for Proposal dated [insert date] and our Bid. We are hereby submitting our Proposal, which includes this Technical Proposal, and a Financial Proposal sealed under a separate envelope.

We confirm that the information contained in our Proposal are correct as of the date of bid submission.

Our Proposal is binding upon us.

We acknowledge and accept the Procuring Entity's right to inspect and audit all records relating to our Proposal irrespective of whether we enter into a contract with the Procuring Entity as a result of this Proposal or not.

We understand you are not bound to accept any Proposal received for the selection of a consultant for the Project.

We acknowledge that failure to sign this Technical Proposal Submission Form and the abovementioned Financial Proposal Submission Form shall be a ground for the rejection of our Proposal.

We remain,

Yours sincerely,

Authorized Signature:  
Name and Title of Signatory:  
Name of Firm:  
Address:

**TPF 2. RELEVANT SERVICES CARRIED OUT IN THE LAST FIVE YEARS THAT BEST ILLUSTRATE QUALIFICATIONS**

Project Name:		Country:
Location within Country:		Professional Staff Provided by Your Firm/Entity(profiles):
Name of Client:		Nº of Staff:
Address:		Nº of Staff-Months; Duration of Project:
Start Date (Month/Year):	Completion Date (Month/Year):	Approx. Value of Services (in Current US\$):
Name of Associated Consultants, if any:		Nº of Months of Professional Staff Provided by Associated Consultants:
Name of Senior Staff (Project Director/Coordinator, Team Leader) Involved and Functions Performed:		
Narrative Description of Project:		
Description of Actual Services Provided by Your Staff:		

**TPF 2. DESCRIPTION OF THE METHODOLOGY AND WORK  
PLAN FOR PERFORMING THE PROJECT**

**TPF 3. TEAM COMPOSITION AND TASKS**

1. Service Delivery Manager		
Name	Position	Tasks
2. Technology Specialists, Two (2)		
Name	Position	Tasks

**TPF 4. FORMAT OF CURRICULUM VITAE (CV) FOR PROPOSED KEY PERSONNEL**

Proposed Position: \_\_\_\_\_

Name of Firm: \_\_\_\_\_

Name of Staff: \_\_\_\_\_

Profession: \_\_\_\_\_

Date of Birth: \_\_\_\_\_

Years with Firm/Entity: \_\_\_\_\_ Nationality: \_\_\_\_\_

Membership in Professional Societies: \_\_\_\_\_

\_\_\_\_\_

Detailed Tasks Assigned: \_\_\_\_\_

\_\_\_\_\_

**Key Qualifications:**

*[Give an outline of staff member's experience and training most pertinent to tasks on project. Describe degree of responsibility held by staff member on relevant previous projects and give dates and locations. Use about half a page.]*

\_\_\_\_\_

**Education:**

*[Summarize college/university and other specialized education of staff members, giving names of schools, dates attended, and degrees obtained. Use about one quarter of a page.]*

\_\_\_\_\_

**Employment Record:**

*[Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of projects. For experience in last ten years, also give types of activities performed and client references, where appropriate. Use about two pages.]*

\_\_\_\_\_

**Languages:**

[For each language, indicate proficiency: excellent, good, fair, or poor in speaking, reading, and writing.]

---

**Certification:**

I, the undersigned, certify that to the best of my knowledge and belief, these data correctly describe me, my qualifications, and my experience.

**Commitment:**

I also commit to work for the Project in accordance with the time schedule as indicated in the contract once the firm is awarded the Project.

\_\_\_\_\_  
[Signature of staff member and authorized representative of the firm] Date: \_\_\_\_\_  
Day/Month/Year

Full name of staff member:  
Full name of authorized representative:

**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. \_\_\_\_\_.

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** \_\_\_\_\_.

**FPF 1. FINANCIAL PROPOSAL SUBMISSION FORM**

*[Date]*

*[Name and address of the Procuring Entity]*

Ladies/Gentlemen:

We, the undersigned, offer to provide the consulting services for *[Title of Project]* in accordance with your Request for Proposals and our Bid (Technical and Financial Proposals). Our attached Financial Proposal is for the sum of *[amount in words and figures]*. This amount is exclusive of the local taxes, which we have estimated at *[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, Ninety (90) calendar days from the opening of the proposals.

We acknowledge and accept the Procuring Entity's right to inspect and audit all records relating to our Bid irrespective of whether we enter into a contract with the Procuring Entity as a result of this Bid.

We confirm that we have read, understood and accept the contents of the Terms of Reference (TOR), the provisions relating to the eligibility of Consultant and the applicable guidelines under RA9184, any and all Bid bulletins issued and other attachments and inclusions included in the Request for Proposal sent to us.

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

We remain,

Yours sincerely,  
Authorized Signature:  
Name and Title of Signatory:  
Name of Firm:  
Address:

**FPF 2. SUMMARY OF COSTS**

Costs	Currency(ies) <sup>3</sup>	Amount in Philippine Peso
Subtotal		
Local Taxes		
Total Amount of Financial Proposal		<hr/> <hr/>

---

<sup>3</sup> *In cases of contracts involving foreign consultants, indicate the exchange rate used.*



## QUALITY-COST BASED EVALUATION PARAMETERS

Quality-Cost Based Evaluation Score Sheet		
CRITERIA	WEIGHT	SCORE
<b>A. TECHNICAL</b>	85.00%	85.00%
<b>A.1. Relevant Experience of the Service Provider</b>	20.00%	20.00%
<i>Number of successfully completed contracts analogous to VAPT services in financial and/ or government institutions within the last 5 years</i>	20.00%	
5 and more contracts	20.00%	
3-4 contracts	15.00%	
1-2 Contracts	10.00%	
No contracts	0.00%	
<b>A.2. Relevant Education and Experience of Key Personnel</b>	40.00%	40.00%
<b>A.2.1. Service Delivery Manager</b>	10.00%	
<b>A.2.1.1. Education</b>	5.00%	
Doctor of Philosophy, related field	5.00%	
Doctor of Philosophy, non-related field	4.75%	
Masteral Degree, related field	4.50%	
Masteral Degree, non-related field	4.25%	
Bachelor's Degree, related field	4.00%	
Bachelor's Degree, non-related field	3.75%	
Non-Bachelor's Degree	0.00%	
<b>A.2.1.2. Experience</b>	5.00%	
<b>A.2.1.2.1. The SDM should have at least three (3) years service delivery or project management experience in handling similar project implementation.</b>	1.00%	
3 years or more experience;	1.00%	
Less than 3 years experience;	0.00%	
<b>A.2.1.2.2. Minimum five (5) years of experience in managing IT projects, <u>and</u> three (3) years of managing information security audits;</b>	2.00%	
Has the minimum required experience;	2.00%	
Less than the minimum required experience;	0.00%	
<b>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</b>	2.00%	
Has the required relevant experience;	2.00%	
Does not have the required relevant experience;	0.00%	

<b>A.2.2. Technology Specialists (2, Averaged)</b>	<b>30.00%</b>	
<b>A.2.2.1. Education</b>	<b>5.00%</b>	
Bachelor's Degree, related field	5.00%	
Bachelor's Degree, non-related field	3.00%	
Non-Bachelor's Degree	0.00%	
<b>A.2.2.2. Experience and Related Training</b>	<b>25.00%</b>	
<b>A.2.2.2.1. Must be permanent employees of the Service Provider</b>	<b>5.00%</b>	
1 year or more work experience with Service Provider;	5.00%	
Less than 1 year work experience;	0.00%	
<b>A.2.2.2.2. Has at least three (3) years experience in information security review or audit especially in conducting network and application layer penetration testing;</b>	<b>5.00%</b>	
Has the minimum required experience;	5.00%	
Less than the minimum required experience;	0.00%	
<b>A.2.2.2.3. Has active certification or at least one of the following: GPEN, LPT, or OSCP;</b>	<b>15.00%</b>	
Has any of the required certification;	15.00%	
Does not have any of the required certification;	0.00%	
<b>A.3. Strict Adherence to the Terms of Reference, or similar Approach and Methodology</b>	<b>25.00%</b>	<b>10.00%</b>
Substance	15.00%	
Completeness	5.00%	
Clarity	5.00%	
<b>B. FINANCIAL</b>	<b>15.00%</b>	<b>15.00%</b>
<b>TOTAL</b>	<b>100.00%</b>	<b>100.00%</b>