



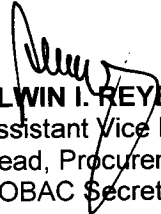
SUPPLEMENTAL/BID BULLETIN NO. 2
For LBP-HOBAC-ITB-CS-20191113-01

PROJECT : **Enterprise IT Security Risk Assessment**
IMPLEMENTOR : **Procurement Department**
DATE : **December 20, 2019**

This Supplemental/Bid Bulletin is issued to modify, amend and/or clarify certain items in the Bid Documents. This shall form an integral part of the Bid Documents.

Modifications, amendments and/or clarifications:

- Section VI (Terms of Reference), and Checklist of the Bidding Documents (Item Nos. 7, 19, 20 & 21 of the Project Technical Component) have been revised. Please see attached revised specific sections of the Bidding Documents.


ALWIN I. REYES, CSSP
Assistant Vice President
Head, Procurement Department and
HOBAC Secretariat

TERMS OF REFERENCE

Enterprise IT Security Risk Assessment

1.0 Name and Description of the Project

Enterprise IT Security Risk Assessment (EITSRA)

Land Bank of the Philippines, "LANDBANK" or "LBP" is a government financial institution whose banking activities are heavily driven by information technology (IT). The emerging IT security threats and vulnerabilities challenge LANDBANK's system of governance, risk management and controls.

In response to business and regulatory requirements and to provide the Board of Directors and Senior Management of LBP a reasonable assurance that the Bank's IT components are operating in a secured environment and controls protecting Bank and customer data are properly aligned with industry standards and best practices, an independent assessment with handholding of technology of the Project identified shall be procured from a competent third party service provider.

The project will be a two-year engagement with the same activities to be performed in each year.

2.0 Objectives of the Project

The proposed project Enterprise Information Technology Security Risk Assessment (EITSRA) requires the assistance of a third party to do an independent assessment of the Bank's IT and data security by undertaking technical reviews such as Penetration Testing (PT), Vulnerability Assessment (VA), and review of compliance to PCI DSS requirements [i.e., Wireless Access Point Assessment, checking of network segmentation, Application Programming Interface Security Assessment, Mobile Application testing, Automated Telling Machine (ATM)/Cash Deposit Machine (CDM) VAPT]. Its primary objectives are the following:

- To identify all existing inherent and potential risks and vulnerabilities related to the Bank's systems, media, devices and facilities (as detailed in Section 3.0 - Scope of Services);
 - To validate the effectiveness and efficiency of the Bank's existing defenses;
 - To review the configuration and security of the Bank's Operating System Platforms, Database Storage and Virtualized environment
 - To recommend action plans and provide handholding on how to mitigate identified risks and vulnerabilities and secure LANDBANK's IT infrastructure from internal and external attacks;
- To conduct presentation to stakeholders (ITCom/RiskCom) of LANDBANK regarding the existing risks facing the bank at the end of each project year.

3.0 Scope of Services

3.1 EITSRA will cover a detailed review of the security risks and controls on the following areas:

- Network Security (e.g., data communication, network equipment, architecture design, segmentation, and firewall rules)
- Platform Security [e.g., Mainframe (IBM Z Series), Linux, AIX, and Windows Systems, Unix]
- Database Security [e.g., Virtual Storage Access Method (VSAM), Oracle, DB2, MySQL, MS SQL, and MongoDB]
- Application Security
- Virtualized Environment Security
- Internet Security (client-facing servers)

3.2 The EITSRA shall focus on the Bank's technology infrastructure that supports the following:

- Microsoft Domain Infrastructure and services
- Remote Access Service
- Domain Name Service
- Application Systems Servers
- Web Servers
- Email Servers
- Proxy Servers
- Anti-virus Servers
- Database Servers
- Internet Banking Application Servers
- Repository/Document Servers
- Routers
- Firewalls and Other Security Devices
- Mobile Facilities

3.3 The EITSRA shall have the following major activities:

Service	Frequency
<p>3.3.1 Internal and External Vulnerability Assessment and Penetration Testing (VAPT)</p> <p>3.3.1.1 Vulnerability assessment and review of network, host and database including at least the following activities:</p> <ul style="list-style-type: none"> • Host Identification – identify various devices comprising the network and server infrastructure. • Server Scan – scan the type of services and which port they are enabled on the identified “live” devices comprising the network. 	<p>Annually</p>

Service	Frequency
<ul style="list-style-type: none"> • Information Retrieval – extract specific information of the device and service configuration and user information to determine the types of vulnerability pertaining to specific device, service and application as well as identifying the appropriate scanning tools to be used. • Vulnerability Scan – use appropriate scanning tools to identify the specific vulnerabilities for each device and system. • Vulnerability Analysis and Validation – evaluate carefully the scanned vulnerabilities and identify possible vulnerability linkages through a detailed analysis of the results. • Assessment of the security configuration - identify specific vulnerabilities in the configuration set up of the Bank's Operating Systems (OS), Database Storage (DB) and Virtualized Environment. • Risk Analysis – risk analysis on identified vulnerability including its impact, likelihood and the corresponding recommendations to mitigate risk. • Manual Review of infrastructure not running on Transmission Control Protocol (TCP) – identify specific vulnerabilities in the Bank's OS, DB not running on TCP. • Handholding with TMG Units concerned to properly remediate vulnerability findings and observations. 	
<p>3.3.1.2 Penetration Testing (PT) of the Bank's network environment:</p> <ul style="list-style-type: none"> • Test from both inside and outside the Bank's network (without and with whitelisting) • Application layer penetration tests • Network layer penetration tests to include components that support network functions as well as operating systems • Conduct retest after exploitable 	Annually

Service	Frequency
vulnerabilities are corrected	
<p>3.3.2 Internal and External VAPT shall cover the following Payment Card Industry Data Security Standards (PCI DSS) Requirements:</p> <p>3.3.2.1 Penetration testing of the Bank's Cardholder Data Environment (CDE)</p> <ul style="list-style-type: none"> • Covers the system components (network devices, servers, computing devices, applications) in the CDE, • Test from both inside and outside the Bank's network • Test after infrastructure or application upgrades (e.g., operating system upgrade, sub-network added to the environment, or a web server added to the environment) • Application layer penetration tests • Network layer penetration tests to include components that support network functions as well as operating systems <p>3.3.2.2 Review all public-facing web applications owned and maintained by LANDBANK via manual or automated application vulnerability security assessment using both authenticated and unauthenticated testing. Include in the assessment, at a minimum, the following vulnerabilities:</p> <p>Re-assess the application after remediation/correction.</p> <p>3.3.2.3 Wireless Access Point Assessment – test the presence of wireless access points and unauthorized wireless access points</p> <p>3.3.2.4 Verify that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in CDE</p>	<p>After any significant change (maximum of 4 times a year)</p> <p>Annually and after any change (maximum of 5 times a year)</p> <p>Quarterly</p> <p>Every six months and after any change to segmentation controls/ methods (maximum of</p>

Service	Frequency
3.3.2.5 Application Programming Interface (API) Security Assessment – determine whether APIs return the correct response (in the expected format) for a broad range of feasible requests; react properly to edge cases such as failures and unexpected/extreme inputs; deliver responses in an acceptable amount of time; and respond securely to potential security attack	5 times a year) Annually and after significant infrastructure or application upgrade (maximum of 5 times a year)
3.3.2.6 Mobile Application Testing – conduct vulnerability assessment and penetration testing on standard security, defense-in-depth, and resiliency against reverse engineering and tampering	Annually and after any change (maximum of 5 times a year)
3.3.2.7 Identify exploitable vulnerabilities on the ATM/CDM <ul style="list-style-type: none"> • Perform a combination of physical and logical attacks • Limit physical attacks to 15 sample ATM/CDM units within Metro Manila 	Annually (No. of ATMs c/o DCAMD)

4.0 Deliverables

The winning Bidder shall deliver the following:

4.1 After every conduct of VAPT, the winning bidder shall deliver the following:

4.1.1 For Penetration Testing

- Executive Summary
- Details of all attacks undertaken, tools used and where applied
- Results of each attack
- Recommendations on how to mitigate these attacks

4.1.2 For Vulnerability Assessment

- Vulnerability Assessment Report (Executive Summary, Conclusion for Management Area, and Specific Action Plans)
- Security Profiling Results (including reports from automated scanning tools)
- Detailed observations and recommendations

- Handholding with TMG Units concerned to properly remediate vulnerability findings and observations

4.1.3 For Internal and External VAPT covering PCI DSS Requirements

- Executive Summary
- Details of all attacks undertaken, tools used and where applied in the CDE
- Results of each attack
- Recommendations on how to mitigate these attacks
- Results of review of public-facing web applications
- Results of Wireless Access Point Assessment
- Results of segmentation methods verification
- Results of Application Programming Interface Security Assessment
- Results of Mobile Application Testing
- Results of ATM/CDM VAPT
- Handholding with TMG Units concerned to properly remediate vulnerability findings and observations

4.1.4 Submit certification or letter that LANDBANK has undergone Enterprise IT Security Risk Assessment based on the overall results with the corresponding rating.

4.1.5 Completely remove applications, software, utilities, and tools used for the vulnerability assessment and penetration testing and submit documentations and/or reports of the removal.

4.2 Winning bidder shall conduct:

- Regular check-point meetings with LANDBANK Project Team,
- Technical presentation to LANDBANK Project Team regarding the results of the penetration test and vulnerability assessment,
- High profile presentation of the results of the engagement and orientation of key stakeholders (ITCom/RiskCom) regarding the existing risks facing the Bank after the completion of the project,

5.0 Documentary Requirements

In addition to those required under Republic Act No. 9184, the technical proposals/bids must include the following required information/documents:

- Detailed Point-by-Point response to Project scope of work and deliverables
- Organizational Chart of the Project
- Project schedule
 - Detailed description of all major tasks/milestones
 - Deliverable items or resource requirements, if any for each of the major tasks

- Delivery Schedule
- Project Schedule (Major Tasks, duration, start and end dates, Gantt Chart) and project status tracking
- List of Projects and Project Team Information using the Project Team Information Form (Annexes A-1 to A-3)
- Assumptions (Constraints and Dependencies)
- LBP Responsibilities (Specific responsibilities relating to resources, skills, infrastructure, documentations, processes, etc., that LBP must satisfy)
- Penetration test and vulnerability assessment approach/methodology
- Tools to be used for the engagement
- Exchange of confidential information and other agreements
- Company Profile

6.0 Other Terms and Conditions

6.1 Proposal Preparation

To be eligible for consideration, the Management Advisory Services Firm must meet all the intent of the scope of work and deliverables. Compliance with the intent of the requirements shall be determined by the LBP HOBAC in accordance with Sections 3.0 and 4.0 of this TOR and on the following:

6.1.1 Point-by-point Response

- The Consulting Firm must submit a point-by-point response from sections 2.0 to 4.0. If no exception, explanation, or clarification is required from its response to a specific item, Consulting Firm shall indicate so in the point-by-point response with the following:

“(Name of Consulting Firm) understands and will comply.”

- Responses similar to “Refer to our literature...” or “Please see www... com” are not acceptable. All materials related to a response must be submitted together with the proposal and not just referenced. Any references in an answer to another location in the TOR materials must indicate the specific page numbers and sections stated in the reference.

6.2 Proposal Submission

- Consulting Firm must submit three (3) sets (one original and two photocopies) of their technical and financial proposals. The authorized representative(s) of a particular bidder is/are required to sign/initial all the documents for authentication.
- Facsimile or electronic submissions are not acceptable

- Compliance with Laws, Policies, Processes, Regulations and Standards

It must, in performance of work under this contract, fully comply with all applicable national or local laws and executive orders

6.3 Contract Contents

This TOR and any addenda, Consulting Firm's responses including any amendments, any best and final offers, and any negotiations shall be included in any resulting contract. Section 4.0 enumerates all the required information and documents that it must submit as part of its proposal to qualify for further consideration, and will serve as basis for any contract between LBP and Consulting Firm.

7.0 Project Timeline

The project must be completed at the end of each project year. The first project year shall be one year from the date of acceptance of Notice to Proceed by the winning bidder. The service provider must therefore provide a project schedule which should show the project milestones and deliverables at each milestone.

All deliverables shall become LANDBANK's property.

8.0 Payment Milestones

Payment Milestone	Deliverables	% of Budget for the Year	
		Year 1	Year 2
Mobilization Fee	Signed Contract	10%	-
Conduct of Internal and External VAPT	Report on results of VAPT	30%	30%
Conduct of Internal and External VAPT to comply with PCI DSS Requirements	Report on results of: 2 Penetration testing of the Bank's Cardholder Data Environment (CDE) 3 Review of public-facing web applications 2 Wireless Access Point Assessments 3 Verification of segmentation methods 3 API Security Assessments 3 Mobile Application Testing 5 ATM/CDM VAPTs	25%	30%
Conduct of Internal	Report on results of	25%	30%

Payment Milestone	Deliverables	% of Budget for the Year	
		Year 1	Year 2
and External VAPT to comply with PCI DSS Requirements	completed conduct of all Internal and External VAPT to comply with PCI DSS Requirements		
Report to Stakeholders	ITCom and RiskCom Report on results of EITSRA activities for the year	10%	10%
Total (inclusive of taxes)		100%	100%

9.0 Project Engagement Team (PET)

- 9.1 Number and Structure – shall be composed of at least five (5) members, with one Project Manager, one Team Leader, and at least 3 Team Members.
- 9.2 Minimum Competencies of the members of the Project Engagement Team (PET) - The Consultant shall send full-time employees who shall possess the qualifications/core competencies indicated in the Short listing Criteria.
- 9.3 The overall Head of the Project Engagement Team must be a Partner/Senior Officer of the consultancy firm/Service Provider.
- 9.4 The Project Engagement Team shall complete the engagement within the prescribed period. In extreme cases where replacement of any of the member is inevitable, the new member must possess the required minimum qualifications/competencies and such replacement shall be subject to the approval of the Head, RMG.

10.0 Approved Budget for the Contract (ABC)

The Approved Budget for the Contract (ABC) is **PHP 22,000,000.00** inclusive of value added tax, all applicable taxes and out-of-pocket expenses. It is understood that all charges to remittance of payment shall be for the account of the Vendor.

11.0 Short Listing

- 1. Minimum score required – 70%
- 2. Short Listing Criteria

ITEMS	WEIGHT	SCORE	MINIMUM REQUIREMENT	DOCUMENT TO BE SUBMITTED												
A. FIRM CREDENTIALS																
<p>1. Has been in the business of information security management advisory services for at least ten (10) years and has completed and/or handled consulting services of size, complexity and technical specialty comparable to proposed project engagement of a Philippine universal/commercial bank/ATM Consortium.</p> <table border="1"> <tr> <td colspan="2">Years in Information Security Management Advisory Services</td> </tr> <tr> <td>>10 years</td> <td>5%</td> </tr> <tr> <td>10 years</td> <td>3%</td> </tr> </table> <table border="1"> <tr> <td colspan="2">Completed 5 Vulnerability Assessment/Penetration Testing Projects</td> </tr> <tr> <td>within the last 5 years</td> <td>25%</td> </tr> <tr> <td>more than 5 years</td> <td>20%</td> </tr> </table>	Years in Information Security Management Advisory Services		>10 years	5%	10 years	3%	Completed 5 Vulnerability Assessment/Penetration Testing Projects		within the last 5 years	25%	more than 5 years	20%	40%		<p>10 years in Information Security Management Advisory services</p> <p>5 completed VAPT projects with Philippine universal/ commercial bank/ATM Consortium</p>	<p>Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK</p> <p>(if with previous similar engagement with LANDBANK, a Certificate of Satisfactory Performance signed by the Business Unit Head concerned shall be submitted)</p>
Years in Information Security Management Advisory Services																
>10 years	5%															
10 years	3%															
Completed 5 Vulnerability Assessment/Penetration Testing Projects																
within the last 5 years	25%															
more than 5 years	20%															
<p>2. Has completed and/or currently handling consulting services of size, complexity and technical specialty comparable to proposed project engagement of an international bank or firm. (combination of the two (2) types of engagement)</p> <table border="1"> <tr> <td>>3 VAPT projects</td> <td>10%</td> </tr> <tr> <td>3 VAPT projects</td> <td>7%</td> </tr> </table>	>3 VAPT projects	10%	3 VAPT projects	7%	10%		<p>3 projects with international bank or firm</p>	<p>Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK</p>								
>3 VAPT projects	10%															
3 VAPT projects	7%															
B. PERSONNEL QUALIFICATION AND NUMBER OF PROJECT ENGAGEMENT TEAM																
<p>1. Project Manager (PM) to be assigned to the project is highly qualified to manage the engagement.</p> <table border="1"> <tr> <td>Exceeds minimum competencies</td> <td>15%</td> </tr> <tr> <td>Meets minimum competencies</td> <td>10%</td> </tr> </table>	Exceeds minimum competencies	15%	Meets minimum competencies	10%	60%		<p>PM has performed and managed 5 engagements comparable to the proposed engagement and has any 2 of the following professional certifications: Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA),</p>	<p>Certification (e.g., CISSP, CISA, CEH, CISM, GPEN, GXPEN, LPT, OSCP, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI)</p>								
Exceeds minimum competencies	15%															
Meets minimum competencies	10%															

ITEMS	WEIGHT	SCORE	MINIMUM REQUIREMENT	DOCUMENT TO BE SUBMITTED						
			Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Global Information Assurance Certification (GIAC) Penetration Tester (GPEN), GIAC Exploit Researcher & Advanced Penetration tester (GXPN), EC Council Licensed Penetration Tester (LPT) Master, Offensive Security Certified Professional (OSCP), Certified Penetration Tester (CPT), Certified Expert Penetration Tester (CEPT), Certified Mobile and Web Application Penetration Tester (CMWAPT), CompTIA PenTest+, Certified Payment Card Industry Security Implementer (CPISI), or other penetration testing-related certifications							
2. Team Lead (TL) to be assigned to the project is highly qualified to manage the engagement. <table border="1" data-bbox="188 1330 576 1458"> <tr> <td>Exceeds minimum competencies</td> <td>15%</td> </tr> <tr> <td>Meets minimum competencies</td> <td>10%</td> </tr> </table>	Exceeds minimum competencies	15%	Meets minimum competencies	10%	15%		TL has functioned as lead in the performance of 4 engagements comparable to the proposed engagement; and has any 2 of the following professional certifications CISSP, CISA, CEH, CISM, GPEN, GXPN, LPT, OSCP, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI)	Certification (e.g., CISSP, CISA, CEH, CISM, GPEN, GXPN, LPT, OSCP, CPT, CEPT, CMWAPT, CompTIA PenTest+, CPISI)		
Exceeds minimum competencies	15%									
Meets minimum competencies	10%									
3. Team Members (TMs) to be assigned to the project are highly qualified to perform the engagement. <table border="1" data-bbox="188 1850 596 2018"> <tr> <td></td> <td>VAPT</td> </tr> <tr> <td>At least two TM exceeds minimum requirements</td> <td>20%</td> </tr> <tr> <td>At least one TM</td> <td>15%</td> </tr> </table>		VAPT	At least two TM exceeds minimum requirements	20%	At least one TM	15%	20%		TM has performed 3 engagements comparable to the proposed engagement; and has any 1 of the following professional certifications CISSP, CISA, CEH, CISM, GPEN, GXPN, LPT, OSCP, CPT, CEPT, CMWAPT, CompTIA PenTest+,	Certification (e.g., CISSP, CISA, CEH, CISM, GPEN, GXPN, LPT, OSCP, CPT, CEPT, CMWAPT, CompTIA PenTest+,
	VAPT									
At least two TM exceeds minimum requirements	20%									
At least one TM	15%									

ITEMS	WEIGHT	SCORE	MINIMUM REQUIREMENT	DOCUMENT TO BE SUBMITTED				
meets minimum requirements			CMWAPT, CompTIA PenTest+, CPISI or other penetration testing-related certifications	CPISI)				
4. Sufficient number of PET to perform the engagement	10%							
<table border="1"> <tr> <td>With more than five (5) personnel</td> <td>10%</td> </tr> <tr> <td>With five (5) personnel</td> <td>7%</td> </tr> </table>	With more than five (5) personnel	10%	With five (5) personnel	7%				
With more than five (5) personnel	10%							
With five (5) personnel	7%							
1 – Project Manager 1 – Team Leader 3 – Team Members								
TOTAL	100%							

Bidders must obtain a minimum score of **70%** for the technical criteria. Only the top five (5) bidders who meet the hurdle rate for the Technical Criteria shall be eligible for the next stage of bidding.

12.0 Bid Evaluation

12.1 Bid Evaluation Procedure – Quality-Cost Based Evaluation/Selection

12.2 Minimum Technical Score – 70%

12.3 Criteria and Rating System

CRITERIA	WEIGHT	RAW SCORE	SCORE	NOTES		
	a	b	ab			
1. TECHNICAL CRITERIA <i>(Firm Credentials, Personnel Competence and Number, and Methodology)</i>	85%					
a. Shortlist Criteria <i>(Firm Credentials, Personnel Competence and Number)</i>	68%			Raw Score based from short listing criteria result.		
b. Methodology Plan of approach and methodology is comprehensive (clear, feasible, timely)	17%			Methodology will be rated in a collegial manner by the TWG.		
<table border="1"> <tr> <td>Criteria: • Methodology and tools to be used are clearly stated • Procedures to be performed are viable, appropriate</td> <td>17%</td> </tr> </table>	Criteria: • Methodology and tools to be used are clearly stated • Procedures to be performed are viable, appropriate	17%				
Criteria: • Methodology and tools to be used are clearly stated • Procedures to be performed are viable, appropriate	17%					

CRITERIA		WEIGHT	RAW SCORE	SCORE	NOTES		
		a	b	ab			
to the size of the organization • Activities are well defined and timelines are explicitly stated and within the timeline of the TOR							
Not Comprehensive	0%						
2. FINANCIAL CRITERIA (PROJECT COST) The proposed bid price of the participating bidder:		15%					
<table border="1"> <thead> <tr> <th>Condition</th> <th>Raw Score</th> </tr> </thead> <tbody> <tr> <td>Lowest Bid</td> <td>15%</td> </tr> <tr> <td>Other Bids</td> <td>SF</td> </tr> </tbody> </table> SF = $.15 * F / F$ Where: SF – score of bid under consideration FI – price of lowest bid F – price of bid under consideration						Condition	Raw Score
Condition	Raw Score						
Lowest Bid	15%						
Other Bids	SF						
GRAND TOTAL		100%					

Checklist of Bidding Documents for Procurement of Consulting Services

Documents should be arranged as per this Checklist. Kindly provide folders or guides, dividers and ear tags with appropriate labels.

First Envelope - Eligibility and Technical Components

- The First Envelope shall contain the following:
 - Eligibility Documents – Class “A”

Legal Eligibility Documents

1. Eligibility Documents Submission Form
2. PhilGEPS Certificate of Registration (Platinum Membership). All documents enumerated in its Annex A must be updated; or
 - Registration Certificate from SEC, Department of Trade and Industry (DTI) for Sole Proprietorship, or CDA for Cooperatives, or any proof of such registration as stated in the Bidding Documents;
 - Valid and current mayor's permit issued by the city or municipality where the principal place of business of the prospective bidder is located; and
 - Tax Clearance per Executive Order 398, Series of 2005, as finally reviewed and approved by the BIR.

Technical Eligibility Documents

3. Duly notarized Omnibus Sworn Statement (sample form - Form No.2)
4. Duly notarized Secretary's Certificate attesting that the signatory is the duly authorized representative of the prospective bidder, and granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the prospective bidder in the bidding, if the prospective bidder is a corporation, partnership, cooperative, or joint venture (sample form - Form No.3).
5. Statement of the prospective bidder of all its ongoing and completed government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid, within the relevant period as provided in the Bidding Documents. The statement shall include all information required in the PBDs prescribed by the GPPB. (sample form - Form No. 1). The duly signed form shall still be submitted even if the bidder has no on-going contract. Copy of Certificate of Satisfactory Performance issued by the Client must also be submitted as proof of satisfactory completion of completed contracts.
6. Bid security in the prescribed form, amount and validity period (ITB Clause 15.1 of the Bid Data Sheet)
7. Form No. 5 – Statement of Consultant's Nationality

Financial Eligibility Documents

8. The prospective bidder's audited financial statements, showing, among others, the prospective bidder's total and current assets and liabilities, stamped “received” by the

BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission.

- Eligibility Documents – Class “B”
 - 9. Valid joint venture agreement (JVA), in case the joint venture is already in existence. In the absence of a JVA, duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful shall be included in the bid. Failure to enter into a joint venture in the event of a contract award shall be ground for the forfeiture of the bid security. Each partner of the joint venture shall submit the legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance.
- Post-Qualification Documents – [The bidder may submit the following documents within five (5) calendar days after receipt of Notice of Post-Qualification]:
 - 10. Business Tax Returns per Revenue Regulations 3-2005 (BIR No. 2550 Q) VAT or Percentage Tax Returns for the last two (2) quarters filed manually or through EFPS.
 - 11. Income Tax Return for 2018 filed manually or through EFPS.

Second Envelope - Project Technical Component

- The Second Envelope shall contain the following:
 1. TPF 1 – Technical Proposal Submission Form
 2. TPF 2 – Experience of the Firm/Consultant References
 3. TPF 3 – Comments and Suggestions of Consultant on the Terms of Reference and on Data, Services, and Facilities to be Provided by the Procuring Entity
 4. TPF 4 – Description of the Methodology and Work Plan for Performing the Project (Penetration test and vulnerability assessment approach/methodology)
 5. TPF 5 – Team Composition and Task
 6. Organizational Chart of the Project
 7. **TPF 6 – Curricula Vitae for Proposed Professional Staff with any of the two (2) following certifications:**
 - **Certified Information System Security Professional (CISSP)**
 - **Certified Information Systems Auditor (CISA) Certified Ethical Hacker (CEH)**
 - **Certified Information Security Manager (CISM)**
 - **Global Information Assurance Certification (GIAC) Penetration Tester (GPEN)**
 - **GIAC Exploit Researcher & Advanced Penetration tester (GXPN)**
 - **EC Council Licensed Penetration Tester (LPT) Master**
 - **Offensive Security Certified Professional (OSCP)**
 - **Certified Penetration Tester (CPT)**
 - **Certified Expert Penetration Tester (CEPT)**
 - **Certified Mobile and Web Application Penetration Tester (CMWAPT)**
 - **CompTIA PenTest+**

- **Certified Payment Card Industry Security Implementer (CPISI)**
 - **Or other penetration testing-related certifications**
8. TPF 7 – Time Schedule for Professional Personnel
 9. TPF 8 – Activity (Work) Schedule
 10. Project Schedule
 - o Detailed description of all major tasks/milestones
 - o Deliverable items or resource requirements, if any for each of the major tasks
 - o Delivery Schedule
 - o Project Schedule (Major Tasks, duration, start and end dates, Gantt Chart) and project status tracking
 11. Form No. 6 – Deliverable Items Summary
 12. Detailed, Point-by-Point Response to Project Objectives and Deliverables
 13. List of Projects and Project Team Information using the Project Team Information Form (Annexes A-1 to A-3).
 14. Assumptions (Constraints and Dependencies)
 15. LBP Responsibilities (Specific responsibilities relating to resources, skills, infrastructure, documentations, processes, etc., that LBP must satisfy)
 16. Tools to be used for the engagement
 17. Exchange of confidential information and other agreements
 18. Company Profile
 19. **Certificate of Satisfactory Performance for all completed projects (as proof that the bidder has been in the business of information security management advisory services for at least 10 years and has completed and/or handled consulting services of size, complexity and technical specialty comparable to proposed project engagement of a Philippine universal/ commercial bank/ATM Consortium.**
 20. **Certificate of Satisfactory Performance for all completed projects as proof that the bidder has completed and/or currently handling consulting services of size, complexity and technical specialty comparable to proposed project engagement of an international bank or firm (combination of the 2 types of engagement).**
 21. **For current and past suppliers of IT security risk assessment for LANDBANK, they must have satisfactory performance in their completed contracts starting in November 2018 onwards. A Certificate of Satisfactory Performance issued by the Head, Information Security and Technology Risk Management Office (ISTRMO) not earlier than thirty (30) calendar days prior to the deadline of submission of bid shall be submitted. The Certificate shall still be subject to verification during post-qualification of bid.**

Note: Certificate of Satisfactory Performance shall be requested in writing from Acting Head, Luciano A. Claudio of ISTRMO (8-405-7283), 31st Floor, LANDBANK Plaza Building, at least five (5) working days prior to the submission of bid.

Third Envelope - Financial Component

- **The Third Envelope shall contain the following:**

The following must be duly filled out and signed by the bidder's authorized representative:

1. FPF 1 – Financial Proposal submission Form
2. FPF 2 – Summary of Costs
3. FPF 3 – Breakdown of Price per Activity
4. FPF 4 – Breakdown of Remuneration per Activity
5. FPF 5 – Travel Expenses, Office Rent, Accommodation and Clerical Assistance per Activity per Activity
6. FPF 6 – Miscellaneous Expenses