

BID BULLETIN NO. 2
For LBP-HOBAC-ITB-GS-20180905-01

PROJECT : **Payment Card Industry Data Security Standard (PCI-DSS) Qualified Security Assessor (QSA) Services**


IMPLEMENTOR : **Procurement Department**

DATE : **October 18, 2018**

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

The modifications, amendments or clarifications are as follows:

- The Terms of Reference (Annex A), Section VII (Specifications) and Checklist of the Bidding Documents (Items 3.j, 3.k, 3.l and 6) have been revised. Please see attached revised Annexes A-1 to A-6 and the specified sections of the Bidding Documents.
- The deadline of submission and the schedule of opening of eligibility/technical and financial documents/proposals for the above project is re-scheduled to **November 8, 2018, 11:00 A.M.** at the Procurement Department, 25th Floor, LANDBANK Plaza Building, 1598 M. H. Del Pilar corner Dr. Quintos Streets, Malate, Manila.



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

Specifications

Specifications	Statement of Compliance
	<p style="text-align: center;">Bidders must state below either “Comply” or “Not Comply” against each of the individual parameters of each specification.</p> <p>Statements of “Comply” or “Not Comply” must be supported by evidence in a Bidders Bid. 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 Bidders 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 provisions of ITB Clause 3.1(a)(ii) and/or GCC Clause 2.1(a)(ii)</p>
<p style="text-align: center;">Payment Card Industry Data Security Standard (PCI-DSS) Qualified Security Assessor (QSA) Services</p> <p>Per attached Revised Terms of Reference (Annexes A-1 to A-6).</p> <p>The following documents shall be submitted inside the eligibility/technical envelope:</p> <ul style="list-style-type: none"> ▪ Certification of Satisfactory Performance (or equivalent document) from at least two (2) banks (local or international) for the conduct of Payment Card Industry Data Security Standard (PCIDSS) compliance/ certification for the past five (5) years (2013 to present) ▪ Certification of Satisfactory Performance (or equivalent document) from at least three (3) institutions (local or international) operating in other industries e.g. publication, manufacturing, telecoms, etc. for the conduct of PCIDSS compliance/ certification for the past five (5) years (2013 to present) ▪ Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as Approved Scanning 	<p>Please state here either “Comply” or “Not Comply”</p>

<p>Vendor (ASV) with validity until the date of submission and opening of bids</p> <ul style="list-style-type: none">▪ Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as QSA with validity until the date of submission and opening of bids▪ Partnership/tie-up agreement (or equivalent document) between local partner and Principal, if applicable▪ Certification of Technical Expert for Certified Information System Security Professional and Certified Ethical Hacker or equivalent.▪ Profiles and certificates of all the project resources▪ Certificate of Satisfactory Performance/ No Delayed Project issued by the Head, Quality Management Department not earlier than thirty (30) calendar days prior to the deadline of submission of bid, if the bidder has existing or completed contract/s with LANDBANK.	
---	--

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Checklist of Bidding Documents for Procurement of Goods and Services

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

The Technical Component (First Envelope) shall contain the following:

1. 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. 7).

2. Duly notarized Omnibus Sworn Statement (sample form - Form No.6).

3. Eligibility requirements

- **Legal Documents**

- 3.a PhilGEPS Certificate of Registration (Platinum Membership). All documents enumerated in its Annex A must be updated; or

- 3.b Class "A" eligibility documents as follows:

- 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 / Financial Documents**

- 3.c Statement of the prospective bidder of all its ongoing 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. 3). This form may no longer be submitted if bidder has no on-going contracts.

- 3.d Statement of the prospective bidder identifying its single largest completed contract similar to the contract to be bid, equivalent to at least fifty percent (50%) of the ABC supported with contract/purchase order, end-user's acceptance or official receipt(s) issued for the contract, 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. 4).
- 3.e 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.
- 3.f The prospective bidder's computation for its Net Financial Contracting Capacity (sample form - Form No. 5).
- 3.g 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.
- 3.h Certification of Satisfactory Performance (or equivalent document) from at least two (2) banks (local or international) for the conduct of Payment Card Industry Data Security Standard (PCIDSS) compliance/certification for the past five (5) years (2013 to present)
- 3.i Certification of Satisfactory Performance (or equivalent document) from at least three (3) institutions (local or international) operating in other industries e.g. publication, manufacturing, telecoms, etc. for the conduct of PCIDSS compliance/certification for the past five (5) years (2013 to present)
- 3.j Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as Approved Scanning Vendor (ASV) with validity until the date of submission and opening of bids**

- 3.k Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as QSA with validity until the date of submission and opening of bids**
- 3.l Partnership/tie-up agreement (or equivalent document) between local partner and Principal, if applicable**
- 3.m Certification of Technical Expert for Certified Information System Security Professional and Certified Ethical Hacker or equivalent
- 3.n Profiles and certificates of all the project resources
- 3.o Certificate of Satisfactory Performance/No Delayed Project issued by the Head, Quality Management Department not earlier than 30 calendar days prior to the deadline of submission of bid, if the bidder has existing or completed contract/s with LANDBANK
- 4. Bid security in the prescribed form, amount and validity period (ITB Clause 18.1 of the Bid Data Sheet);
- 5. Schedule VI - Schedule of Requirements with signature of bidder's authorized representative.
- 6. Revised Section VII – Specifications with response on compliance and signature of bidder's authorized representative.**
- 7. Post-Qualification Documents – (Non-submission of the following documents during the bidding date shall not be a ground for the disqualification of the bidder).
 - 7.a 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 the BIR EFPS; and
 - 7.b Income Tax Return for 2017 filed manually or through the BIR EFPS

The Financial Component (Second Envelope) shall contain the following:

- 1. Duly filled out Bid Form signed by the bidder's authorized representative (sample form - Form No.1)
- 2. Duly filled out Schedule of Prices signed by the bidder's authorized representative (sample form - Form No.2)

TERMS OF REFERENCE

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) QUALIFIED SECURITY ASSESSOR (QSA) SERVICES

1. INTRODUCTION

Land Bank of the Philippines is required by Visa and MasterCard to be Payment Card Industry - Data Security Standard (PCI DSS) certified to ensure that the cardholder's information is secured.

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data.

The acquisition of a Qualified Security Assessor (QSA) aims to facilitate the certification of LANDBANK to PCI-DSS standards.

2. OBJECTIVES OF THE PROJECT

2.1 The engagement of a QSA aims to:

- a. Facilitate LBP certification against PCI DSS standards;
- b. Perform audit/scanning of LBP's systems, products, services, personnel and processes to identify the scope of the certification;
- c. Review necessary documentation and policies.

3. FIRM CREDENTIALS

3.1 The QSA local partner or its Principal must comply with the following:

- a. Have obtained PCI DSS Certification for at least two (2) banks (local or international) in the past five (5) years (2013 to present); and
- b. Have obtained PCI DSS Certification for at least three (3) institutions (local or international) operating in other industries e.g., publication, manufacturing, telecoms, etc. in the past five (5) years (2013 to present).

3.2 Documentary Requirements:

- a. Certification of Satisfactory Performance (or equivalent document) from at least two (2) banks (local or international) for the conduct of PCIDSS compliance/certification for the past five (5) years (2013 to present)
- b. Certification of Satisfactory Performance (or equivalent document) from at least three (3) institutions (local or international) operating in other industries e.g., publication, manufacturing, telecoms, etc. for the conduct of PCI DSS compliance/certification for the past five (5) years (2013 to present)
- c. **Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as approved scanning vendor**

(ASV) with validity until the date of submission and opening of bids.

- d. **Printout of webpage of the PCI Security Standards Council official website or equivalent document where the name of the vendor or its partner is included as QSA with validity until the date of submission and opening of bids.**
- e. Partnership/**tie-up** agreement (or equivalent document) between local partner and Principal, if applicable

3.3 The QSA shall create a Project Team composed of at least one (1) full time Project Manager, one (1) Technical Expert, one (1) Process Analyst and one (1) Quality Assurance Analyst.

3.3.1 The Team must possess the following qualifications:

a. Project Manager

- Should have a solid understanding of the banking industry and with experience in assessing similar industry and should be a certified PCI DSS QSA;
- At least three (3) years of experience as Project Manager in PCI DSS and/or PA DSS related projects; and
- Familiar with the different banking systems including policies and procedures issued by Bangko Sentral ng Pilipinas (BSP), BancNet, Mastercard, and Visa.

b. Technical Expert

- Familiar with the various banking application systems, security software and network devices;
- With certification for CISSP and Certified Ethical Hacker or equivalent
- Proficient and with direct involvement in at least two (2) previous engagements in performing the ASV scanning.

**Qualification of other team members may be determined by the Project Manager*

3.3.2 In extreme cases where replacement of any member of the team is unavoidable, the new member must possess the qualifications provided in this Terms of Reference (TOR). The replacement must be communicated by the Project Manager to the LBP PCI DSS Technical Working Group (TWG)/Steering Committee at least thirty (30) days prior to the execution of the change, for evaluation and approval.

3.3.3 The QSA Project Team must ensure the completion of the engagement within the agreed period. Should a change in timeline be necessary, the Project Manager must request in writing for its extension, to be endorsed by the LBP PCI DSS TWG/Steering Committee for HOBAC approval.

The QSA Project Team shall submit profiles and certificates of all the project resources.

4. SCOPE OF QSA SERVICES

- 4.1 The Audit Plan to be used shall include the following required elements:
- Project Plan (Project Schedule)
 - Project Status Report
 - Issue Form/Action Tracker, if necessary

Phase	Deliverables	Completion Criteria
I. Project Initiation and Planning	1. Overall Project Management Plan <ul style="list-style-type: none"> • Project Plan (Project Schedule) • Team Structure 	1. The Overall Project Management Plan should be: <ul style="list-style-type: none"> a. aligned with project objectives and shall at least specify: <ul style="list-style-type: none"> • Overall project approach - detailed approach and methodology • Scope of services and timelines • Participating LBP units and required facilities, equipment, and other logistic requirements • Project assumptions, dependencies and constraints b. Presented during kick-off meeting c. Approved by PCI-DSS Technical Working Group (TWG) 2. Monthly Summary Report/Project Status Report on completed activities and deliverables should be reviewed, approved/ signed off by PCI-DSS TWG/Steering Committee
II. Assessment	1. ASV Scan Report 2. AOSC (Attestation of Scan Compliance) 3. Issue Tracker	1. Approved Scanning Vendor (ASV) to perform external vulnerability scan (ASV Scan) for PCI DSS scoped systems, quarterly. 2. The ASV Scan to be

Phase	Deliverables	Completion Criteria
	for Document Review 4. Issue Tracker for ASV Scan 5. Prioritized Approach 6. Status Letter	conducted until LBP achieves a Pass Scan or until 5 passes. 3. QSA to review all necessary documentation offsite and provides necessary recommendation in Issue Tracker. 4. Monthly Summary Report/Project Status Report on completed activities and deliverables should be reviewed, approved/ signed off by PCI-DSS TWG/Steering Committee
III. Audit Pass 1	1. Report on Compliance (ROC); 2. Issue Tracker (if any findings are noted) 3. Status Letter	1. Vendor to audit the LANDBANK against latest version of PCI DSS Standard. 2. Issuance of Status Letter and/or PCI DSS Certificate. 3. Issue Tracker and Results of QSA Audit should be noted and accepted by PCI-DSS TWG/Steering Committee 4. Submission and Presentation of phase summary/ project status report on completed activities and deliverables 5. Issue tracker must be detailed to cover all the necessary elements of Audit findings (including PCI DSS Requirement, Physical Location, system IP, Interviewed person, Document Name, Recommendations etc.)
IV. Audit Pass II	4. Report on Compliance (ROC); 5. Issue Tracker (if any findings are noted) 6. Status Letter	1. Vendor to audit the LANDBANK against latest version of PCI DSS Standard. 2. Issuance of Status Letter and/or PCI DSS Certificate. 3. Issue Tracker and

Phase	Deliverables	Completion Criteria
		<p>Results of QSA Audit should be noted and accepted by PCI-DSS TWG/Steering Committee</p> <p>4. Submission and Presentation of phase summary/ project status report on completed activities and deliverables</p> <p>5. Issue tracker must be detailed to cover all the necessary elements of Audit findings (including PCI DSS Requirement, Physical Location, system IP, Interviewed person, Document Name, Recommendations etc.)</p>
IV. Audit Support Service	<p>1. Assistance in providing recommendation on PCI DSS Audit Results</p> <p>2. Conduct of Quarterly ASV Scans</p>	<p>1. Provide recommendation on Process Improvement in line with payment card Operations.</p> <p>2. Continuance of quarterly ASV Scan.</p> <p>3. The ASV Scan to be conducted until LBP achieves a Pass Scan or until 5 passes.</p>

5. PROJECT TIMELINE

- Twelve (12) months from the Signing of Contract. However, Service Provider maybe allowed extension of project timeline provided delays incurred is attributable to the Bank.

6. APPROVED BUDGET FOR THE CONTRACT

- The Approved Budget for the Contract (ABC) is PhP3,710,000.00 (or USD\$70,000.00 computed at P53.00=\$1, rounded off), inclusive of the 12% Value-Added Tax and other incidental and logistical expenses.**

7. PAYMENT MILESTONES

Payment Milestone	% of Contract Price
Mobilization fee	15%
Assessment (ASV Scans) Deliverable: AOSC, Document Review	20%

Completion of Audit	40%
Audit Pass 1 -----20% deliverable : ROC, AOC, Status Letter, Certificate, Issue Tracker (if any gaps are noted)	
Audit Pass 2 -----20% deliverable : ROC, AOC, Status Letter, Certificate	
Audit Support (ASV Scans)	25%

8. NO PRICE ESCALATION

There shall be no price escalation allowed within the term of the contract.