



BID BULLETIN NO. 2
For LBP-HOBAC-ITB-CS-20170627-02

PROJECT : Enterprise Information Technology Security Risk
Assessment and Information Security Awareness
Assessment


IMPLEMENTOR : Procurement Department

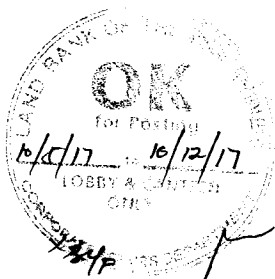
DATE : October 5, 2017

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:

- Section V (Terms of Reference) and Checklist of the Bidding Documents (Item 3 of the Technical Information/Documents) 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



1.0 Name and Description of the Project

Enterprise IT Security Risk Assessment and Information Security Awareness Assessment

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 its employees are aware of their information security responsibilities, an independent assessment with handholding of technology of the Project identified shall be procured from a competent third party service provider.

2.0 Objectives of the Project

The proposed project requires the assistance of a third party to do an independent assessment of the Bank's IT security by undertaking a technical review such as Penetration Testing (PT), Vulnerability Assessment (VA) and Information Security Awareness Assessment (ISAA) of LANBANK employees, service company workers, and employees of other third party service providers. 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 on how to mitigate the identified risks and secure LANDBANK from internal and external attacks;
 - To assess information security level of awareness (e.g., on social engineering, phishing) of LANBANK employees, service company workers, and employees of other third party service providers.
 - To handhold/transfer to LANDBANK information security office personnel the methodology of assessing information security awareness and technology in conducting vulnerability assessment.
 - To conduct presentation to stakeholders of LANDBANK regarding the existing risks facing the bank after the completion of the project.
-

3.0 Scope of Services

- 3.1 Penetration testing of the Bank's network environment from various access points to be performed by the Penetration Testing (PT) Team independently from the Vulnerability Assessment (VA) Team:
- Internet
 - Intranet
- 3.2 Vulnerability assessment and review of network, host and database including at least the following activities:
- 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.
 - 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 of technology with ISTRMO personnel of the Bank.
- 3.3 Enterprise IT Security Risk Assessment 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 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 and MS SQL]
 - Virtualized Environment Security
 - Internet Security (client-facing servers)
 - Handholding of technology with ISTRMO personnel of the Bank
-

3.4 The review will specifically focus on the Bank's technology infrastructure that supports the following applications:

- 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
- External Routers
- Firewalls
- **Mobile Facilities**

3.5 Test subjects for the conduct of information security awareness assessment shall include LBP officers and employees, and employees of service providers assigned at the Bank (Head Office and Field Units) thru:

3.5.1 External Social Engineering Security Assessment – use of publicly available sources such as websites, search engines, and DNS records to obtain employee names, titles, phone numbers, email addresses and/or a list provided by the Bank of at least 200 test subjects that can be used for the following activities:

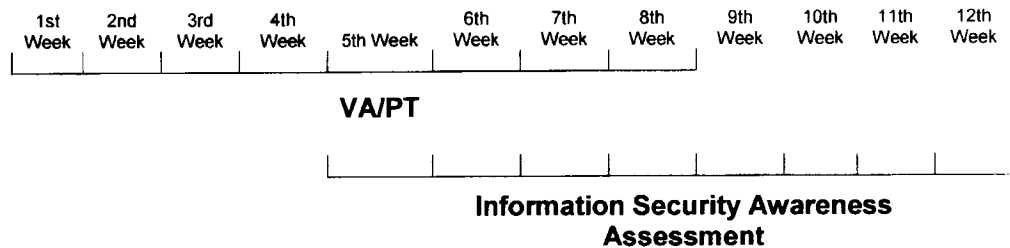
- Phone-based – make phone calls to individuals within the organization to induce the employee to divulge sensitive information over the phone in violation of Bank policies
- Targeted Email Phishing Attack – send emails to individuals and groups (may include credit card clients) within the organization to entice the user to click on an external link that will either attempt to gather sensitive information
- **Face-to-face Attack – in person and onsite harvesting of information**

3.5.2 Internal Social Engineering Security Assessment – assess vulnerability of at least 200 test subjects thru the following:

- Attempt unauthorized entry through tailgating or alternate entrances
 - Check for unsecured computers
 - Report computers left unattended and logged in
 - Discover sensitive materials left unsecured
 - Check random work stations for security issues
 - Examine workspace for exposed passwords
 - Search printer, fax and copier areas for confidential material
 - Examine trash bins and dumpsters for improperly discarded
-

- information
- Provide data analysis of the results of assessment with corresponding recommendations
- **Assess the adequacy of the Bank's existing information security awareness trainings**
- Design security awareness training materials appropriate for different employees (e.g., new hires, IT personnel, security guards, service providers)

3.6 Conduct of the vulnerability assessment, penetration testing and information security awareness assessment shall be done for a period of at most 3 months.



4.0 Deliverables

The winning Bidder shall deliver the following:

- 4.1 At the end of the engagement, 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, Information Security Roadmap and Specific Action Plan)
 - Security Profiling Results (including reports from automated scanning tools)
 - Handholding of technology with ISTRMO of the assessment of configuration and security of the Bank's Operating System [e.g., Mainframe (IBM Z Series), Linux, AIX, and Windows Systems, Unix], Database Storage (VSAM, Oracle, MS SQL) and Virtualized Environment

- Handholding of technology with ISTRMO personnel of the manual review of infrastructure not running on Transmission Control Protocol (TCP) – identify specific vulnerabilities in the Bank's OS, DB not running in TCP.
- Detailed observations and recommendations

4.1.3 For Information Security Awareness Assessment

- Executive Summary
- Details of social engineering attacks performed
- Results of each attack
- Recommendations on how to respond and mitigate these attacks
- Materials for security awareness trainings

4.1.4 Submit certification that LANDBANK has undergone Enterprise IT Security Risk Assessment and Information Security Awareness Assessment based on the overall result 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,
- Presentation of the results of conduct of security awareness assessment,
- High profile presentation of the results of the engagement and orientation of key stakeholders of LANDBANK 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, objectives and deliverables
- Draft Contract
- 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 (Annex A)
- 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
- Information Security Awareness 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 to all numbered sections, subsections, appendices, annexes and attachments of the TOR. 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.”

- It must organize its proposal into sections following the format of this TOR, with tabs separating each section;
 - In case its proposal does not comply with the specified proposal format, or is difficult to understand, reads or lacks any of the requested information, the proposal will be returned for immediate revision; and
 - 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 within a twelve-week period from the 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 Project Engagement Team (PET)

- 8.1 Number and Structure – shall be composed of at least seven (7) members, with one Project Manager, one leader and one member for each project component.

| Project Manager | |
|-----------------------------------|--|
| <i>Penetration Testing</i> | <i>Vulnerability Assessment</i> |
| Leader (1) | Leader (1) |
| Member/s (at least 1) | Member/s (at least 1) |

| Information Security Awareness Assessment |
|---|
| Leader (1) |
| Member/s (at least 1) |

- 8.2 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.
- 8.3 The Team Leader to be assigned in the conduct of information security awareness assessment with handholding shall direct/supervise the team to be provided by the Bank to conduct the engagement.
- 8.4 The overall Head of the Project Engagement Team must be a Partner of the consultancy firm/Service Provider.
- 8.5 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.

9.0 Approved Budget for the Contract (ABC)

The Approved Budget for the Contract (ABC) is PHP _____ 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.

10.0 Short Listing

- 1. Hurdle Rate to be met – 70%
- 2. Short-listing Criteria

| ITEMS | WEIGHT | SCORE | MINIMUM REQUIREMENT | DOCUMENT TO BE SUBMITTED | | | | | | | | | | | | | | | | | | | | |
|--|---|-------|---|--------------------------|-----------------------------------|-----|-----------|----|-----------|--|---|--|-------------|-----|--------------|----|-----------|----|-----------|----|-----|--|--|---|
| C. FIRM CREDENTIALS | 40% | | | | | | | | | | | | | | | | | | | | | | | |
| <div>3. 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.</div> <div><table><tr><th colspan="2">Vulnerability Assessment/ Penetration Testing</th></tr><tr><td>>5 projects</td><td>20%</td></tr><tr><td>2-5 projects</td><td>15%</td></tr><tr><td>1 project</td><td>5%</td></tr><tr><td>0 project</td><td>0%</td></tr></table><table><tr><th colspan="2">Information Security Awareness Assessment</th></tr><tr><td>>3 projects</td><td>10%</td></tr><tr><td>2-3 projects</td><td>5%</td></tr><tr><td>1 project</td><td>2%</td></tr><tr><td>0 project</td><td>0%</td></tr></table></div> | Vulnerability Assessment/ Penetration Testing | | >5 projects | 20% | 2-5 projects | 15% | 1 project | 5% | 0 project | 0% | Information Security Awareness Assessment | | >3 projects | 10% | 2-3 projects | 5% | 1 project | 2% | 0 project | 0% | 30% | | | <div>Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK</div> <div>(if with previous engagement with LANDBANK, a Certificate of Satisfactory Performance signed by the Unit Head shall be submitted)</div> |
| Vulnerability Assessment/ Penetration Testing | | | | | | | | | | | | | | | | | | | | | | | | |
| >5 projects | 20% | | | | | | | | | | | | | | | | | | | | | | | |
| 2-5 projects | 15% | | | | | | | | | | | | | | | | | | | | | | | |
| 1 project | 5% | | | | | | | | | | | | | | | | | | | | | | | |
| 0 project | 0% | | | | | | | | | | | | | | | | | | | | | | | |
| Information Security Awareness Assessment | | | | | | | | | | | | | | | | | | | | | | | | |
| >3 projects | 10% | | | | | | | | | | | | | | | | | | | | | | | |
| 2-3 projects | 5% | | | | | | | | | | | | | | | | | | | | | | | |
| 1 project | 2% | | | | | | | | | | | | | | | | | | | | | | | |
| 0 project | 0% | | | | | | | | | | | | | | | | | | | | | | | |
| <div>4. 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)</div> <div><table><tr><td>>3 projects (equal number of engagements, e.g., 2 VAPT/ 2 ISAA)</td><td>10%</td></tr><tr><td>2-3 projects (combination of engagements e.g., 2 VAPT/1 ISAA)</td><td>5%</td></tr><tr><td>1 project (any of the engagement)</td><td>2%</td></tr></table></div> | >3 projects (equal number of engagements, e.g., 2 VAPT/ 2 ISAA) | 10% | 2-3 projects (combination of engagements e.g., 2 VAPT/1 ISAA) | 5% | 1 project (any of the engagement) | 2% | 10% | | | <div>Certificate of Satisfactory Performance for all completed projects stated in the list to be submitted to LANDBANK</div> | | | | | | | | | | | | | | |
| >3 projects (equal number of engagements, e.g., 2 VAPT/ 2 ISAA) | 10% | | | | | | | | | | | | | | | | | | | | | | | |
| 2-3 projects (combination of engagements e.g., 2 VAPT/1 ISAA) | 5% | | | | | | | | | | | | | | | | | | | | | | | |
| 1 project (any of the engagement) | 2% | | | | | | | | | | | | | | | | | | | | | | | |
| D. PERSONNEL QUALIFICATION AND NUMBER OF PROJECT ENGAGEMENT TEAM | 60% | | | | | | | | | | | | | | | | | | | | | | | |

| ITEMS | WEIGHT | SCORE | MINIMUM REQUIREMENT | DOCUMENT TO BE SUBMITTED | | | | | | |
|--|------------------------------|-------|----------------------------|--------------------------|-----------------------|----|-----|--|--|---|
| <p>5. Project Manager (PM) to be assigned to the project is highly qualified to manage the engagement.</p> <table><tr><td>Exceeds minimum competencies</td><td>15%</td></tr><tr><td>Meets minimum competencies</td><td>10%</td></tr><tr><td>Less than the minimum</td><td>0%</td></tr></table> | Exceeds minimum competencies | 15% | Meets minimum competencies | 10% | Less than the minimum | 0% | 15% | | PM has performed and managed 5 engagements comparable to the proposed engagement and has any 2 of the following professional certification: Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), ISO 27001 Lead Auditor/Lead Implementer | Certification (i.e., CISA, CISM, CISSP, CEH, ISO 27001 LI/LA) |
| Exceeds minimum competencies | 15% | | | | | | | | | |
| Meets minimum competencies | 10% | | | | | | | | | |
| Less than the minimum | 0% | | | | | | | | | |
| <p>6. Team Leader (TL) to be assigned to the project is highly qualified to perform the engagement.</p> <table><tr><td>Exceeds minimum competencies</td><td>15%</td></tr><tr><td>Meets minimum competencies</td><td>10%</td></tr><tr><td>Less than the minimum</td><td>0%</td></tr></table> | Exceeds minimum competencies | 15% | Meets minimum competencies | 10% | Less than the minimum | 0% | 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 certification CISSP, CISA, CEH, CISM, ISO 27001 LA/LI | Certification (i.e., CISA, CISM, CISSP, CEH, ISO 27001 LI/LA) |
| Exceeds minimum competencies | 15% | | | | | | | | | |
| Meets minimum competencies | 10% | | | | | | | | | |
| Less than the minimum | 0% | | | | | | | | | |

| ITEMS | WEIGHT | SCORE | MINIMUM REQUIREMENT | DOCUMENT TO BE SUBMITTED | | | | | | | | | | | | | | | | | | | |
|--|------------------------------|-------|----------------------------|--------------------------|-----------------------|----|-----------------|--|--|---|------------|------------|-----------------------|-----------------------|---|--|------------|--|-----------------------|--|-----|--|--|
| <p>7. Team Member (TM) to be assigned to the project is highly qualified to perform the engagement.</p> <table><tr><td>Exceeds minimum competencies</td><td>20%</td></tr><tr><td>Meets minimum competencies</td><td>15%</td></tr><tr><td>Less than the minimum</td><td>0%</td></tr></table> | Exceeds minimum competencies | 20% | Meets minimum competencies | 15% | Less than the minimum | 0% | 20% | | Each TM has performed 3 engagements comparable to the proposed engagement and has any 1 of the following professional certification CISSP, CISA, CEH, CISM, ISO 27001 LA/LI | Certification (i.e., CISA, CISM, CISSP, CEH, ISO 27001 LI/LA) | | | | | | | | | | | | | |
| Exceeds minimum competencies | 20% | | | | | | | | | | | | | | | | | | | | | | |
| Meets minimum competencies | 15% | | | | | | | | | | | | | | | | | | | | | | |
| Less than the minimum | 0% | | | | | | | | | | | | | | | | | | | | | | |
| <p>8. Sufficient number of PET to perform the engagement</p> <table><tr><td>With more than 7 personnel</td><td>10%</td></tr><tr><td>With 7 personnel</td><td>5%</td></tr><tr><td>Less than 7 personnel</td><td>0%</td></tr></table> <table><tr><td colspan="2">Project Manager</td></tr><tr><td>Penetration Testing</td><td>Vulnerability Assessment</td></tr><tr><td>Leader (1)</td><td>Leader (1)</td></tr><tr><td>Member/s (at least 1)</td><td>Member/s (at least 1)</td></tr><tr><td colspan="2">Information Security Awareness Assessment</td></tr><tr><td colspan="2">Leader (1)</td></tr><tr><td colspan="2">Member/s (at least 1)</td></tr></table> | With more than 7 personnel | 10% | With 7 personnel | 5% | Less than 7 personnel | 0% | Project Manager | | Penetration Testing | Vulnerability Assessment | Leader (1) | Leader (1) | Member/s (at least 1) | Member/s (at least 1) | Information Security Awareness Assessment | | Leader (1) | | Member/s (at least 1) | | 10% | | |
| With more than 7 personnel | 10% | | | | | | | | | | | | | | | | | | | | | | |
| With 7 personnel | 5% | | | | | | | | | | | | | | | | | | | | | | |
| Less than 7 personnel | 0% | | | | | | | | | | | | | | | | | | | | | | |
| Project Manager | | | | | | | | | | | | | | | | | | | | | | | |
| Penetration Testing | Vulnerability Assessment | | | | | | | | | | | | | | | | | | | | | | |
| Leader (1) | Leader (1) | | | | | | | | | | | | | | | | | | | | | | |
| Member/s (at least 1) | Member/s (at least 1) | | | | | | | | | | | | | | | | | | | | | | |
| Information Security Awareness Assessment | | | | | | | | | | | | | | | | | | | | | | | |
| Leader (1) | | | | | | | | | | | | | | | | | | | | | | | |
| Member/s (at least 1) | | | | | | | | | | | | | | | | | | | | | | | |
| TOTAL | 100% | | | | | | | | | | | | | | | | | | | | | | |

11.0 Bid Evaluation

11.1 Bid Evaluation Procedure – Quality-Cost Based Evaluation/Selection 11.2 Criteria and Rating System

| CRITERIA | WEIGHT | RAW SCORE | SCORE | NOTES | | | | |
|---|---|-----------|-------------------|---|--|--|--|--|
| | a | b | ab | | | | | |
| 3. TECHNICAL CRITERIA (Firm Credentials, Personnel Competence and Number, and Methodology) | 85% | | | | | | | |
| c. Shortlist Criteria (Firm Credentials, Personnel Competence and Number) | 68% | | | Raw Score based from short listing criteria result. | | | | |
| d. Methodology Plan of approach and methodology is comprehensive (clear, feasible, timely) | 17% | | | Methodology will be rated in a collegial manner by the TWG. | | | | |
| <table><tr><td>Criteria:<ul style="list-style-type: none">Methodology and tools to be used are clearly statedProcedures to be performed are viable, appropriate to the size of the organizationActivities are well defined and timelines are explicitly stated and within the timeline of the TOR</td><td>17%</td></tr><tr><td>Not Comprehensive</td><td>0%</td></tr></table> | Criteria: <ul style="list-style-type: none">Methodology and tools to be used are clearly statedProcedures to be performed are viable, appropriate to the size of the organizationActivities are well defined and timelines are explicitly stated and within the timeline of the TOR | 17% | Not Comprehensive | 0% | | | | |
| Criteria: <ul style="list-style-type: none">Methodology and tools to be used are clearly statedProcedures to be performed are viable, appropriate to the size of the organizationActivities are well defined and timelines are explicitly stated and within the timeline of the TOR | 17% | | | | | | | |
| Not Comprehensive | 0% | | | | | | | |

| CRITERIA | WEIGHT | RAW SCORE | SCORE | NOTES | | | | | | |
|---|------------------|------------------|------------|-------|------------|----|-----|--|--|--|
| | a | b | ab | | | | | | | |
| <p>4. FINANCIAL CRITERIA (PROJECT COST)</p> <p>The proposed bid price of the participating bidder:</p> <table border="1"><tr><td>Condition</td><td>Raw Score</td></tr><tr><td>Lowest Bid</td><td>15%</td></tr><tr><td>Other Bids</td><td>SF</td></tr></table> <p>SF = .15*FI/F</p> <p>Where: SF – score of bid under consideration FI – price of lowest bid F – price of bid under consideration</p> | Condition | Raw Score | Lowest Bid | 15% | Other Bids | SF | 15% | | | |
| Condition | Raw Score | | | | | | | | | |
| Lowest Bid | 15% | | | | | | | | | |
| Other Bids | SF | | | | | | | | | |
| GRAND TOTAL | 100% | | | | | | | | | |

ANNEX A

**Project Engagement
TERMS OF REFERENCE**

**Project Team Information
(PROJECT ROLE)**

(Surname, First Name, Middle Name)

I. Responsibilities: (Enumerate the details)

II. Educational Attainment:

| NAME OF INSTITUTION /SCHOOL | PERIOD OF ATTENDANCE | DIPLOMA/DEGREE EQUIVALENT | AWARDS/ DISTINCTIONS RECEIVED |
|--------------------------------|-------------------------|------------------------------|-------------------------------------|
| | | | |
| | | | |
| | | | |
| | | | |

III. Work/Project Experience

| JOB TITLE | WORK DESCRIPTION | COMPANY | PERIOD COVERED |
|-----------|------------------|---------|-------------------|
| | | | |
| | | | |
| | | | |
| | | | |

IV. Certifications

| Certification Title | Year Acquired |
|---------------------|---------------|
| | |
| | |
| | |

V. Proficiency (Provide certificate and other documents to support your answers)

| | |
|---|--|
| 1. Number of years of being a constituent partner/employee of the third party service provider. | |
| 2. Number of years of actual experience in providing the proposed project engagement for any institution. | |
| 3. Number of years of actual experience in providing the proposed project engagement for the banking institution. | |
| 4. Number of years of direct involvement or participation in the proposed project engagement in a local universal bank and/or any reputable international bank | |
| 5. Number of projects with direct involvement or participation in the proposed project engagement for a local universal bank and/or any reputable international bank. <i>(please specify type of participation, e.g., member, TL, PM)</i> | |

Response to Request for Information (RFI)

| CONSULTING FIRM | COMPANY'S BRIEF DESCRIPTION | ESTIMATED DURATIONS (MONTHS) | CONSULTING FEE |
|----------------------------|------------------------------------|---|---------------------------|
| A | | | |
| B | | | |
| C | | | |

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.

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.5).
2. Duly notarized Omnibus sworn statement (sample form - Form No.4).
3. Eligibility requirements
 - **Legal Document**
 - 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. 1). The duly signed form shall still be submitted even if the bidder has no on-going contract.

- 3.d The prospective bidder's computation for its Net Financial Contracting Capacity (sample form - Form No. 3).
- 3.e 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.
4. Bid security in the prescribed form, amount and validity period (ITB Clause 18.1 of the Bid Data Sheet);

The SECOND ENVELOPE shall contain the following Technical Information/Documents

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 Revised 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
 5. TPF 5 – Team Composition/Project Engagement Team and Tasks
 6. TPF 6 – Curriculum Vitae for Proposed Professional Staff
 7. TPF 7 – Time Schedule for Professional Personnel
 8. TPF 8 – Activity (Work) Schedule
 9. Detailed Point-by-Point response to Project scope of work, objectives and deliverables
 10. Draft Contract
 11. Organizational Chart of the Project
 12. 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
 13. List of Projects and Project Team Information using the Project Team Information Form (Annex A)
 14. Assumptions (Constraints and Dependencies)
-

15. LBP Responsibilities (Specific responsibilities relating to resources, skills, infrastructure, documentations, processes, etc., that LBP must satisfy)
16. Penetration test and vulnerability assessment approach/methodology
17. Information Security Awareness Assessment approach/methodology
18. Tools to be used for the engagement
19. Exchange of confidential information and other agreements
20. Company Profile

**The THIRD ENVELOPE shall contain the following
Information/Documents:**

1. Duly filled out FPF1 and FPF2 duly signed by the bidder's authorized representative.
-