

**SUPPLEMENTAL/BID BULLETIN NO. 1
For LBP-ICTBAC- ITB-GS-20240916-02**


PROJECT: Three (3) Years Subscription to Digital Risk Protection Management Security Platform

DATE: 13 November 2024

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:

1. Response to prospective bidders/clarifications per attached Annex H.
2. Section VII. Technical Specifications (pages 43-44), Checklist of the Bidding Documents (pages 67-70) and Terms of Reference (Annexes D1 – D6) have been revised. Copies of said revised portions of the Bidding Documents are herein attached.
3. The bidders are reminded that the deadline of Bid Submission and Opening is on 20 November 2024 at 10:00 AM. **Late bids shall not be accepted.**
4. The bidders are encouraged to use the Bid Securing Declaration as Bid Security.


SVP MARILOU L. VILAFRANCA
Chairperson, ICT-BAC

Technical Specifications

Specifications	Statement of Compliance
<p>Three (3) Years Subscription to Digital Risk Protection Management Security Platform</p> <ol style="list-style-type: none">1. Minimum technical specifications and other requirements per attached Revised Terms of Reference (Annexes D-1 to D-6)2. The documentary requirements enumerated in Revised Annexes D-4 to D-5 of the Terms of Reference shall be submitted in Eligibility and Technical Component to support the compliance of the Bid to the technical specifications and other requirements. <p>Non-submission of the above documents may result in the post-disqualification of the bidder.</p>	<p>Bidders must signify their compliance to the Technical Specifications/Terms of Reference by stating below either "Comply" or "Not Comply".</p> <p>Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the 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 applicable laws and issuances.</p> <p>Please state here either "Comply" or "Not Comply"</p>

Conforme:

Name of Bidder

Signature over Printed Name of
Authorized Representative

Position

Checklist of Bidding Documents for Procurement of Goods and Services

The documents for each component should be arranged as per this Checklist. Kindly provide guides or dividers with appropriate labels.

Eligibility and Technical Component (PDF File)

- ***The Eligibility and Technical Component shall contain documents sequentially arranged as follows:***

- **Eligibility Documents – Class “A”**

Legal Eligibility Documents

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

Technical Eligibility Documents

2. 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; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder. (sample form - Form No. 7).
3. 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 last five (5) years from the date of submission and receipt of bids. The statement shall include all information required in the sample form (Form No. 3).
4. Statement of the prospective bidder identifying its Single Largest Completed Contract (SLCC) similar 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 sample form (Form No. 4).

Financial Eligibility Documents

5. 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.
6. The prospective bidder's computation for its Net Financial Contracting Capacity (NFCC) following the sample form (Form No. 5), or in the case of Procurement of Goods, a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

o **Eligibility Documents – Class “B”**

7. Duly signed 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 its legal eligibility documents. The submission of technical and financial eligibility documents by any of the joint venture partners constitutes compliance, provided, that the partner responsible to submit the NFCC shall likewise submit the statement of all its ongoing contracts and Audited Financial Statements.
8. For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos, Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.
9. Certification from the DTI if the Bidder claims preference as a Domestic Bidder.

o **Technical Documents**

10. Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
11. Section VI – Schedule of Requirements with signature of bidder's authorized representative.
12. **Section VII – Revised Specifications with response on compliance and signature of bidder's authorized representative.**
13. Duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).

Note: During the opening of the first bid envelopes (Eligibility and Technical Component), only the above documents will be checked by the BAC if they are all present using a non-discretionary “pass/fail” criterion to determine each bidder's compliance with the documents required to be submitted for eligibility and the technical requirements.

o **Other Documents to Support Compliance with Technical Specifications [must be submitted inside the first bid envelope (Eligibility and Technical Component)]**

14. Duly filled-out **Revised Terms of Reference** signed in all pages by the authorized representative/s of the bidder.
15. Securities and Exchange Commission (SEC) Registration as proof that the bidder has at least five (5) years of existence in the IT industry.
16. Manufacturer's authorization (sample form - Form No. 9) or its equivalent document, confirming that the bidder is authorized to provide the brand being offered and consumables supplied by the manufacturer, including any warranty obligations and after sales support as may be required.
17. List of at least two (2) local Certified Information Technology engineer with at least three (3) years work experience and have handled the proposed platform/solution for at least one (1) year and must submit the following documents:
 - Certificate of Employment;
 - Resume/Curriculum Vitae;
 - List of Trainings/Seminars (including proposed solution/project related seminars); and
 - Two (2) Certifications in Cybersecurity.
18. **Certificate of Employment, Resume/Curriculum Vitae and List of Projects handled [including client/company name, project name and project duration (start date and end date)] of a dedicated Project Manager employed with the bidder with at least three (3) years work experience as a project manager for the proposed solution.**
19. Certificate of Employment, Resume/Curriculum Vitae and List of Projects handled as a Success Manager [including client/company name, project name and project duration (start date and end date)] of a designated Success Manager employed by the Manufacturer.
20. List of at least two (2) installed based in the Philippines, with one (1) Financial/Insurance or Government Institution, of the same digital risk management platform being offered or similar solution such as security awareness tool with client name, contact person, complete address, contact number and email address.
21. Detailed Escalation Procedure and Support Plan Flow Chart including contact numbers and email addresses.
22. Business Continuity Plan (BCP) that will support the operations of a Commercial or Universal Bank, and List of updated Technical Support Unit including name, contact number, and email address.

23. Reference documents or website link to verify that the proposed solution is a globally recognized Third (3rd) Party Market Research and Advisory Firms (e.g. Garner Magic Quadrant) as a leaders or challengers for the year 2023.
24. White paper or similar reference documents on the correlation of security ratings (scores) with relative likelihood of breach.

○ **Post-Qualification Documents/Requirements – [The bidder may submit the following documents/requirements within five (5) calendar days after receipt of Notice of Post-Qualification]:**

25. 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.
26. Latest Income Tax Return filed manually or through EFPS.
27. Original copy of Bid Security (if in the form of a Surety Bond, submit also a certification issued by the Insurance Commission).
28. Original copy of duly notarized Omnibus Sworn Statement (OSS) (sample form - Form No.6).
29. Duly notarized Secretary's Certificate designating the authorized signatory in the Contract Agreement if the same is other than the bidder's authorized signatory in the bidding (sample form – Form No. 7).

Financial Component (PDF File)

• ***The Financial Component shall contain documents sequentially arranged as follows:***

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).
3. Duly filled out Bill of Quantities Form signed by the bidder's authorized representative (Annex E)

Note: The forms attached to the Bidding Documents may be reproduced or reformatted provided the information required in the original forms and other requirements like signatures, if applicable, are complied with in the submittal.

November 07, 2024

Technical Specifications and Terms of Reference for the Three (3) years Subscription to Digital Risk Protection Management Security Platform

Objective: To provide externally observed security risk monitoring and benchmarking data for use in assessing the security posture of bank and its third-party suppliers/vendors.

Item	Description	Comply	Remarks
General Requirements			
1	The offered solution and/or services must be a SaaS platform.		
2	Must not require installation of any software such as agents, clients; and/or hardware of any type, in the environment of the organization and third-parties organization to be monitored.		
3	Must have the capability to provide all (if required) of the following from within a single platform: i) Continuous monitoring of the organization and third-parties organization ii) Automate workflow for 3rd Party Vendor Onboarding & Validation iv) Perform Quantification of Financial Impact of Cyber Risk iv) Provides a search engine to help identify, contextualize, and prioritize critical threats across global attack surface.		
4	Must offer an uptime services commitment of 98% or more for a given month during the term of the subscription.		
5	Must have a built-in multi-factor authentication for the sign in process.		
Data Transparency/Accuracy			
6	The solution should be a signatory of Principles for Fair and Accurate Security Ratings from reputed business federations and associations.		
7	The solution should allow and has a process for rated organizations submit corrections and remediations to improve their rating.		
8	The solution should be able to provide statistics about their accuracy when requested.		
9	The solution should provide a methodology whitepaper discussing how their solution works.		
Cybersecurity Risk Ratings			
10	Must include continuous monitoring for at least 15 Domains with cybersecurity risk ratings.		
11	Must provide a cybersecurity risk ratings platform that enables the bank to assess and manage our own cybersecurity posture. The cybersecurity risk ratings platform should has the ability to generate risk ratings, identify security gaps, and provide remediation guidance.		
12	Must provide a cybersecurity risk ratings platform that enables to assess and manage the bank third-party vendors/business partners. The cybersecurity risk ratings platforms must have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.		
13	The platform must be able to generate an Initial score for a company new to the cybersecurity risk ratings platform in minutes rather than hours or days.		

14	The platform must allow the bank to self-service to create portfolio to segment organizations into one or more portfolios to help manage <i>groups of organizations to align with a specific project or role.</i>		
16	The platform must allow the bank to self-service to organize portfolios in groups to assess their overall risk.		
17	The platform must allow the bank to self-service to have granular visibility into the risk posture of our individual business units, subsidiaries, and other types of organizational structures by building our own custom scope for cybersecurity risk ratings and get a detailed rating on-demand.		
Benchmarking			
18	The platform must allow the bank to benchmark its own organization's cybersecurity posture against industry peers, competitors, or other organizations.		
19	The platform must allow the bank to benchmark its own organization and / or other organizations potential security issues that has been detected against one of several recognized information security frameworks available.		
20	These recognized information security framework includes but not limited to: <ul style="list-style-type: none"> • ISO/IEC 27001:2022 • NIST CSF • SOC2 		
21	The platform must be able support to showcase the bank's compliance evidence, browse compliance evidence for any organization, or request evidence from an organization.		
Risk Factors			
22	The platforms data collection should include but not limited to the following risk factors: <ul style="list-style-type: none"> • Network Security • DNS Health • Patching Cadence • Endpoint Security • IP Reputation • Application Security • Cubit Score • Hacker Chatter • Information Leak • Social Engineering 		
23	The platform must provide simple rating system to provide a clear and easy-to-understand view of an organization's cybersecurity posture.		
Digital Footprints/Assets			
24	The solution and/or services should create a Digital Footprint of the bank internet-facing assets as it collects and analyses cybersecurity signals and calculates the bank cyber risk rating.		
25	The solution and/or services should provide visualization of all the assets that have been attributed to the bank, organized by IP addresses, IP ranges, domains, and geographic distribution.		
26	The platform detection methods must include but not limited to: <ul style="list-style-type: none"> • DNS Lookup • Port Scan 		

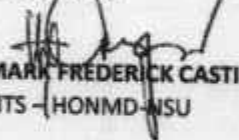
	<ul style="list-style-type: none"> • Published Data • User Input • Platform Login • Third-party • WHOIS 		
27	The platform must allow the bank to self-validate their Digital Footprints via review, claim, manage and add assets.		
28	For manage assets, the platform must review the submitted request by the bank within 72 hours. Once the platform approve it, the ratings scores should updates within approximately 48 hours after approval.		
Alerts, Event Logs and Reporting			
29	The platform should be able to automate monitoring for score changes based on numerical thresholds and grade drops and raises and receive notifications in-app and via email.		
30	The platform must be able to generate, view, and share reports from the cybersecurity risk ratings platform.		
31	The platform must be able to generate at least 3 (THREE) types of reports: Summary, Issues, or Detailed Report		
32	The platform must be able to schedule future sending of a generated report.		
33	The platform must provide a transparency into score changes with a historical score chart.		
34	The platform must have an event log that provides further transparency around score fluctuations with clear record of issue changes and their impact on overall grade.		
35	<p>The platform event logs must covers:</p> <ul style="list-style-type: none"> • New findings: newly detected findings for issues added • Resolved findings: findings for issues the company resolved internally • Decayed findings: findings for issues that no longer impact the score • Security events: breaches, incidents, etc 		
36	The platform must allow the bank to build or automatically generate a plan to improve LANDBANK score while providing full transparency into how specific security issues impact LANDBANK score.		
Integration			
37	The platform must have integration with leading Integrated Risk Management, Third Party Risk Management, and/or Vulnerability Management vendors. Must provide the list of technology and integration partner.		
38	The platform must make available API service and must have a proper documentation for API integration.		
39	The platform must provide an automated questionnaire and evidence exchange platform that automatically provides insight into the validity of questionnaire responses		
Third Party Questionnaires			
40	The platform must provide an automated questionnaire and evidence exchange platform that automatically provides insights into the validity of questionnaire response		
41	<p>The platform must have an automated questionnaire and evidence exchange platform, and must support the following:</p> <ul style="list-style-type: none"> • Questionnaire: Upload or create a custom questionnaire template or choose from a list of industry standard template questionnaires. 		

	<ul style="list-style-type: none"> • Send: Send questionnaire to one vendor or multiple vendors at once. With options to send once or recurring schedules • Track: Track the status of every questionnaire, see due dates, and see turnaround time of all the questionnaires. Supports automatic reminders. • Validate: Once a questionnaire is done, there should be email notification and the questionnaire and attachments can be reviewed. The engine of this platform should maps cybersecurity risk ratings to individual responses, allowing the bank to trust and verify questionnaire responses. 		
Other Requirements			
42	The supplier must comply with the requirements in relation to Third Party/Vendor Assessment conducted by the Bank internal audit and external audit such as Bangko Sentral ng Pilipinas (BSP), Commission on Audit (COA), etc		
42	The supplier must notify the bank IT personnel of any critical security vulnerability, firmware upgrade and performance patches and fixes that is needed to be applied. The supplier must provide detailed support plan and procedure.		
44	The supplier must notify the bank IT personnel of any related security incidents such as, but not limited to compromise/breaches involving the vendor/supplier/client data, the product hardware or software, etc. It must be reported within a risk-informed time frame of at-least 24 hours upon knowledge or discovery of the incident. The supplier must provide documentation on incident response handling procedure.		
45	The supplier must provide knowledge transfer training on the proposed solution for at-least five (5) LBP IT personnel within 60 calendar days. The supplier must submit training certificate.		
46	The supplier through the product vendor should conduct/provide at least five (5) Third Party Risk Management related certification courses to LANDBANK.		
47	The supplier must provide Three (3) years Warranty on Product and Services. Services must also cover any reconfiguration/integration after successful implementation.		
48	The supplier shall be subjected to Performance Assessment regularly. The results of the Performance Assessment shall be considered in the renewal of the contract. The performance assessment of the winning bidder shall also be considered upon them entering into other contracts with the Bank.		
Bidder's Eligibility Requirements			
49	Securities and Exchange Commission (SEC) Registration as proof that the bidder has at least five (5) years of existence in the IT industry.		
50	The bidder must be an authorized reseller or distributor of the brand being offered. The bidder must submit certification from the principal.		
51	<p>The bidder must have at least two (2) local Information Technology (IT) engineers to support the re-configurations and provide online/onsite support. The bidder must submit the following:</p> <ul style="list-style-type: none"> • Certificate of employment (must have at-least 3 years of work experience and have handled the proposed platform/solution for at-least a year) • Resume or Curriculum Vitae 		

	<ul style="list-style-type: none"> List of trainings and seminars attended (including the proposed solution/project related seminar) Must also have at-least two (2) Certification in Cybersecurity such as (but not limited to) ISC2, CompTIA Security+, GIAC Security Essential, CISA, CEH, OSCP, SSCP and other related security certifications. 		
52	<p>The bidder must have a dedicated Project Manager (PM) employed with the bidder to oversee the project. The bidder must submit the following:</p> <ul style="list-style-type: none"> Certificate of Employment (must have at least three (3) years work experience as a project manager for the proposed solution.) Resume or Curriculum Vitae List of the Project handled, include the End-User/Client company name, Project Name and Project Duration (start date and end date). 		
53	<p>The bidder must have a designated Success Manager employed by the Manufacturer and should be the single point of contact for the onboarding, conduct operational training and portal walkthrough at the end of onboarding. The bidder must submit the following:</p> <ul style="list-style-type: none"> Certificate of Employment for the assigned personnel indicating the date of hire. Curriculum Vitae or Resume List of the Project handled as a Success Manager, including the End-User/Client company name, Project Name and Project Duration (start date and end date). 		
54	<p>The bidder must have at-least two (2) installed bases of the same digital risk management platform being offered or similar solution such as security awareness tool, wherein one (1) is a Financial / Insurance or Government institutions. Must submit list of installed bases with client name, contact person, address, telephone number and email address.</p>		
55	<p>The bidder must have a local Helpdesk to provide 24 x 7 technical assistance. The Bidders must submit the escalation procedure and support plan flow chart/details.</p>		
56	<p>The bidder must submit Business Continuity Plan (BCP) that will support the operations of a Commercial or Universal Bank, and List of Updated Technical Support (include name, contact numbers, and email address.</p>		
57	<p>The bidder must provide reference documents or website link to verify that the proposed solution is a globally recognized Third (3rd) Party Market Research and Advisory Firms (e.g. Gartner Magic Quadrant) as a leaders or challengers for the year 2023.</p>		
58	<p>The bidder solution should provide white paper or similar reference documents on the correlation of security ratings (scores) with relative likelihood of breach</p>		
Delivery/Contract Period			
59	<p>Three (3) years license subscription to start upon receipt of Notice to Proceed.</p>		
Payment Terms and Condition			
60	<p>Payable Annually for Three (3) years</p>		
61	<p>The following documentary requirements for payment shall be submitted:</p>		

	<ul style="list-style-type: none"> • Sales invoice/Billing Statement/Statement of Account on or before the 15th day after every delivery • Delivery Receipt with printed name and signature of LANDBANK employee who received the delivery and actual date of receipt of items; and • Warranty Certificate specifying the period covered by the warranty (if applicable) <p>The Supplier shall be paid within sixty (60) calendar days after submission of sales invoice or claim and complete documentary requirements.</p>		
62	<p>Pursuant to Malacañang Executive Order No. 170 (Re: Adoption of Digital Payments for Government Disbursements and Collections) issued on 12 May 2022, directing all government agencies to utilize safe and efficient digital disbursement in the payment of goods, services and other disbursements, all payments for this Contract shall be through direct credit to the supplier's deposit account with LANDBANK. Thus, the supplier shall maintain a deposit account with any LANDBANK Branch where the proceeds of its billings under this Contract shall be credited.</p>		

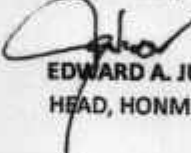
Evaluated by:


MARK FREDERICK CASTILLO
 SITS - HONMD-NSU

Checked by:


JAY-R G. JADREN
 ITO, HONMD-NSU

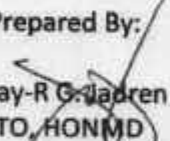
Approved by:

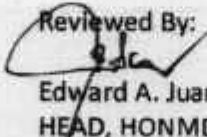

EDWARD A. JUAN
 HEAD, HONMD

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS

RESPONSES TO BIDDER'S QUERIES AND/OR SUGGESTIONS DATE	November 07, 2024
PROJECT IDENTIFICATION NO.	LBP-ICTBAC-ITB-GS-20240916-02
PROJECT NAME	Three (3) Years Subscription to Digital Risk Protection Management Security Platform
PROPONENT UNIT/TECHNICAL WORKING GROUP	Head Office Network Management Department

ITEM NO.	PORTION OF BIDDING DOCUMENTS	QUERIES AND /OR SUGGESTIONS	LANDBANK'S RESPONSES
52	<p>The supplier must have a dedicated Project Manager (PM) employed with the bidder to oversee the project. The bidder must submit the following:</p> <ul style="list-style-type: none"> • Certificate of Employment (must have at least three (3) years work experience as a Success Manager for the proposed solution. • Resume or Curriculum Vitae • List of the Project handled, include the End-User/Client company name, Project Name and Project Duration (start date and end date). 	<p>Please verify if the work experience pertains to Project Manager instead of the Success Manager written in the TOR</p> <p>Also, if this is for a Project Manager should the work experience be based on any IT related projects like Network and Security?</p>	<p>Yes., work experience should be as a Project Manager for IT Network and Security related projects.</p>

Prepared By:

 Jay-R G. Jaoren
 ITO, HONMD

Reviewed By:

 Edward A. Juan
 HEAD, HONMD