EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022

Expression of Interest (EOI)

Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)

December 2022

Contents

SBP BANKING SERVICES CORPORATION

Request for Expression of Interest (REOI)

EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022

SBP Banking Services Corporation, on behalf of State Bank of Pakistan (SBP), invites Expression Of Interest (EOI) from the firms that are on Active Taxpayers List of the Federal Board of Revenue to conduct the ***IT Security Review of Business Applications (DWH/DAP Platform).*** Bidding will be conducted pursuant to *Regulation-3 (B) - Quality and Cost Based Selection (QCBS)* method of Procurement of Consultancy Services Regulations, 2010.

Expressions of Interest (EOI) Documents containing detailed Terms & Conditions etc. may be obtained free of cost upon submission of an email request at gsd.proc2@sbp.org.pk or can be directly downloaded from SBP website at www.sbp.org.pk. In case of any discrepancy/conflict, provisions of EOI Documents including any addenda posted on the procuring agency website, shall prevail.

A pre-submission meeting will be held on **December 28, 2022 at 11:00 AM (PKT)** via Zoom Meeting Application. Meeting ID & Password is given in the EOI Documents. The prospective firms can also obtain the Meeting ID & Passcode through an email request at gsd.proc2@sbp.org.pk

The Expression of Interest, prepared in accordance with the instructions provided in the EOI Documents must be delivered in a hard copy submitted (in person, or by post) at the address given below on or before **January 09, 2023 at 11:00 AM (PKT)** which shall be opened on the same day at **11:30 AM (PKT)** at Learning Resource Centre, State Bank of Pakistan, I.I. Chundrigar Road, Karachi, Pakistan in the presence of representatives of firms who may choose to be present. This Letter of Invitation is also available on websites: www.sbp.org.pk & www.ppra.org.pk

Joint Director
Procurement Division-II
General Services Department
4th Floor, BSC House, State Bank of Pakistan
I.I Chundrigar Road, Karachi
Tel: (021) 3311-5420/5423
Email: gsd.proc2@sbp.org.pk

SECTION II – INSTRUCTIONS TO APPLICANTS

<table>
<tr><th colspan="2">A. General</th></tr>
<tr><td>1. Scope of Expression of Interest (EOI)</td><td>1.1. State Bank of Pakistan – hereinafter referred to as the “Client”, having its principal place of business at I.I. Chundrigar Road, Karachi, Pakistan, wherever the context requires shall be deemed to include its subsidiaries invites sealed Interests for <u>Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)</u></td></tr>
<tr><td>2. Qualification & Eligibilities of Applicant</td><td>2.1. The Consultancy Firm (hereinafter referred to as the “Applicant”) fulfilling the following criteria is eligible to participate in the procurement process.

<u>Shortlisting Criteria,</u>
<table>
<tr><th>Sr.#</th><th>Evaluation Parameter</th><th>Means of Verification</th></tr>
<tr><td>1.</td><td>The Applicant must appear on the Active Tax Payers List of FBR.</td><td>Proof of ATL and copy of Tax Registration Certificate or other sufficient documentary proof.</td></tr>
<tr><td>2.</td><td>The Applicant must be registered/incorporated in Pakistan</td><td>Certificate of Registration/Incorporation or other sufficient documentary proof.</td></tr>
<tr><td>3.</td><td>The Applicant must never have been blacklisted or debarred by any organization and is not in the sanctioned list of NACTA (National Counter Terrorism Authority).</td><td>Affidavit on stamp paper of Rs. 100/- as per format given under Section IX.</td></tr>
<tr><td>4.</td><td>Relevant Experience: The Applicant must have completed at least (05) similar assignments in Financial Industry or other similar organizations

Note: Only “Penetration Testing” or “VA/PT” of web application or network components will not be considered as a similar assignment.</td><td>Relevant Supporting Documents/Copies of Completion Certificates / NOA/ PO /Copies of the contracts/ Sufficient documentary proof for experience.</td></tr>
</table></td></tr>
<tr><td>3. One EOI per Applicant</td><td>3.1. The Applicant shall submit only one EOI. Joint Venture or Sub-Consultancy is not allowed.</td></tr>
<tr><td>4. Cost of EOI</td><td>4.1. The Applicant shall bear all costs associated with the preparation and submission of its EOI, and the Client will in no case be responsible or liable for such costs whether or not the Applicant qualify for the award of contract.</td></tr>
<tr><td>5. Contents of EOI</td><td>5.1. The contents of EOI Documents are listed below. These should be read in conjunction with any addenda that may be issued before the closing date.
i. Letter of Invitation
ii. Instructions to Applicants
iii. Eligibility/Qualification Criteria
iv. Terms of Reference
v. Guidelines for Submission of Interests
vi. Letter of Submission of Interest
vii. Authorization Form For Applicant’s Representative</td></tr>
</table>

	viii. Applicant Information Form ix. Format of Undertaking
6. Amendment of EOI Documents	6.1. At any time before the deadline for submission of EOI, the Client may, for any reason, whether at its initiative or in response to a clarification requested by an Applicant, amend the EOI documents. Amendments will modify or replace/supersede earlier ones. 6.2. Amendments will be provided in the form of *Addenda* to the EOI documents, which will be sent in writing to all the Applicants in receipt of the EOI documents from the Client. Addenda will be binding on the Applicants and they will be required to immediately acknowledge receipt of any such Addenda. It will be assumed that the amendments contained in such Addenda will have been taken into account by the Applicant in its EOI. 6.3. To allow the Applicants reasonable time to take the amendment into account in preparing their EOI, the Client may, at its discretion, extend the deadline for the submission of EOI.
7. Pre-submission meeting	7.1. Pre-submission meeting will be held on **December 28, 2022, 11:00 AM (PKT)** via Zoom Meeting Application. Details of the meeting are given as; • **Meeting Link:** https://zoom.us/j/3338347786?pwd=U3liTzZNald0MStIOEZEa1U5QlJxUT09 • **Meeting ID:** 333 834 7786 • **Passcode:** abc123
B. Preparation of Interests	
8. Language of EOI	8.1. The EOI prepared by the Applicants, as well as all the correspondence and documents relating to the EOI, exchanged by the Applicant and the Client shall be written in English or Urdu.
9. Documents Comprising the EOI	9.1. The EOI submitted by the Applicants shall comprise all the documents to establish their Eligibility/ Qualification including incorporation/ registration documents as per prevailing laws which includes but is not limited to copies of incorporation certificates, tax registration certificates, active taxpayer proof, etc. The successful Applicant will ensure compliance with all relevant local tax laws including necessary registration if required.
C. Submission of Interests	
10. Sealing & Marking of EOI	10.1. The Applicants shall submit one original and two copies of EOI documents, in separate envelopes; duly marked the envelopes as **"ORIGINAL EXPRESSION OF INTERESTS DOCUMENTS"** and **"COPY NO. [number]."**
11. Deadline for Submission of EOI	11.1. EOI must be received by the Client by the time and at the address specified in the Letter of Invitation.
12. Late Submission of EOI	12.1. The Client will not entertain the EOI received after the prescribed deadline.
D. Evaluation of Interests	

13. Evaluation and Comparison of EOI	13.1. Pursuant to Evaluation Criteria contained in these documents, EOIs submitted by the Applicants as per Guidelines for Submission of EOI (Section V) shall be evaluated in detail as per eligibility criteria given in Section III. 13.2. Under the provision of Rule 48 of PPR 2004, any applicant may file its written complaint against the eligibility parameters or any other terms and conditions as prescribed in the EOI Documents, if found contrary to the provisions of the procurement regulatory framework, the same shall be addressed by the Grievance Redressal Committee (GRC) before the EOI submission deadline. The details of Grievance Redressal Committee (GRC) is given on the PPRA website: www.ppra.org.pk.
14. Issuance of Request for Proposal Documents	14.1. Only shortlisted Applicants will be issued the Request for Proposal (RFP) documents soliciting sealed Technical and Financial Proposals under *Regulation-3 (B) Quality and Cost Based Selection Method* of the Procurement of Consultancy Services Regulations, 2010 (PCSR-2010). 14.2. It is mandatory for the shortlisted firm to submit Technical and Financial proposals against the Request for Proposal (RFP) documents. In case of non-submission of Technical and Financial proposals, the Clint reserves the right to debar the firm for future procurements for a minimum period of six months.
15. Overriding Effect of	15.1. Whenever there is any conflict in these documents with the stipulations of Public Procurement Rules,2004 (Rules) and Procurement of Consulting Service Regulations,2010 (Regulations) the Rules shall prevail.

SECTION III – ELIGIBILITY/QUALIFICATION CRITERIA

The Evaluation of Expression of Interests will be ascertained based on the following parameters:-

Sr.#	Evaluation Parameter	Means of Verification
1.	The Applicant must appear on the Active Tax Payers List of FBR.	Proof of ATL and copy of Tax Registration Certificate or other sufficient documentary proof.
2.	The Applicant must be incorporated/Registered in Pakistan,	Certificate of Registration/Incorporation or other sufficient documentary proof.
3.	The Applicant must never have been blacklisted or debarred by any organization and is not in the sanctioned list of NACTA (National Counter Terrorism Authority).	Affidavit on stamp paper of Rs. 100/- as per format given at **Section IX.**
4.	**Relevant Experience:** The Applicant must have completed at least (05) similar assignments in Financial Industry or other similar organization Note: Only "Penetration Testing" or "VA/PT" of web application or network components will not be considered as a similar assignment.	Relevant Supporting Documents/Copies of Completion Certificates / NOA/ PO /Copies of the contracts/ Sufficient documentary proof for experience.

Note:

1. The shortlisted Applicant will be issued the Request for Proposal (RFP) documents soliciting sealed Technical and Financial Proposals under *Regulation-3 (B) Quality and Cost Based Selection Method* of the Procurement of Consultancy Services Regulations, 2010 (PCSR-2010).
2. The EOI should be submitted in sealed envelopes.
3. Only the EOI submitted in hard form will be entertained.

SECTION IV – TERMS OF REFERENCE

1. Objective

An independent cybersecurity risk assessment/ analysis of business applications for identification of security vulnerabilities & control weaknesses and provide appropriate recommendations to remediate/ mitigate identified risks to further improve the overall cyber security posture.

2. Scope of Assignment

Data Warehouse (DWH) System / DAP Platform of the Bank, comprised of multiple IT systems with associated network components as given below. Further details and number of the systems will be provided in the technical RFP.

Systems to be reviewed includes:

a) Application Servers
b) Database Servers
c) Operating Systems
d) Web Applications
e) Network Components like N/W Firewalls, IDS/IPS & VPN Client etc.

3. Requirement for Security Assessment

3.1. The applicant at minimum shall objectively review the following domains in order to evaluate the current security posture and provide domain wise issues along with security recommendations respectively.

a) Application hosting and architecture
b) Interfaces and integration with other applications
c) Privileged and Standard Users Account Management
d) Authentication, Authorization and Access Management
e) Custom Application Development and Application change management process
f) Configuration security assessment of application & its underlying Operating System
g) Configuration security assessment of database & its underlying Operating System
h) Configuration security assessment of network components including Firewalls, IDS/IPS, NAC, VPN and MFA setups.
i) File & Data Integrity and Security Controls
j) Data and system classification
k) Auditing, Logging and Monitoring
l) System & Data Backup Management
m) Business continuity and disaster recovery
n) Software Vulnerability & Patch Management
o) Cryptographic Keys & Digital Certificates Management
p) Software Quality Assurance (SQA) process review
q) Documentation (Policy, SOPs & user manual etc.)
r) Any other area the applicant considers important or requested by the client during engagement.

3.2. Vulnerability Assessment and Penetration Testing (Tools Based Activity)
Applicant will perform the following activities on the application environment provided by the client of each in scope system at client's premises:

a) Vulnerability assessment of application on production or equivalent environment.
b) Penetration testing (Grey box) of application on production or equivalent environment.

4. Work plan and Methodology

a) Applicant will adopt a systematic and structural approach during this engagement in order to discover all possible systems and their associated components subject to the defined rules of engagement for identifying vulnerabilities and associated risks.

b) The applicant will provide outlines of the plan for the main activities / tasks of the assignment, their content and duration, phasing and milestones (including any interim approvals by the Client), and tentative delivery dates of the reports. The proposed work plan should be consistent with the technical approach and methodology, showing understanding of the TOR and ability to translate them into a feasible working plan.

5. Work Requirement

a) During engagement, the applicant will ensure complete privacy of the client's information. Data and any information related to the client and its IT systems will not be allowed to leave client's premises in any form.

b) Security Assessment and Penetration testing should be performed in an appropriate manner to avoid potential impacts on the operations or security of the business applications.

c) Entire security assessments will be performed onsite i.e. atClient's physical premises at its Karachi office.

d) Licensing of any proprietary security tool will be the responsibility of the applicant. The execution of any security tool/script on the client's network or any associated component will require client's prior review and approval.

e) Use of any pirated, cracked, unlicensed software, tool or script will not be allowed.

f) The actual information related to IP addresses and other required information will be shared with the successful bidder only.

6. Project Completion Timeline

a) Client expects that entire project should be completed within 16 calendar weeks or early starting from the date of commencement of contract agreement.

b) Any change in the project completion timeline will be subject to the justifications provided by the applicant under the normal working circumstances and its acceptance by the client.

7. Project Deliverables

Following two reports in accordance to section 3.1 and 3.2 should be delivered:

a. Vulnerability Assessment & Penetration Testing Report
b. Security Assessment Report

Further, each report should include all the requirements for security assessment as mentioned in section 3.1 and 3.2 but not limited to, the following information.

a. Executive Summary
b. Brief on work plan and methodology
c. Scope description
d. Overview of existing environment
e. Findings (analysis of risk, impact and its rating inline to Bank's Enterprise Risk Management (ERM) framework)
f. Recommendation for remediation (with literature references where applicable)

Note:

- *All reports will be treated as "Confidential" and will be provided to authorized person of the client only. Initial report marked as DRAFT will be provided in electronic format for review of the client. The client's authorized person will review the draft in line with project scope and will assess whether the report covers all aspects of the scope as provided in terms of reference. The client will also review the completeness and quality of the report in terms of its contents, references and supporting documents.*

- *After fulfilling the requirements/gaps specified by the client, if any, the applicant would submit final copy of the reports to the client's authorized person for acceptance.*

8. Non-Disclosure Agreement

a) The applicant must ensure complete confidentiality of theclient's information. All information obtained during this engagement by the applicant and its affiliates will be subject to non-disclosure for lifetime. The client, after completion of the assignment may request the applicant to destroy/delete all the information obtained during the assignment.

b) The applicant will sign a non-disclosure agreement (NDA) with the client for which the client will provide draft copy of the NDA for signing off.

c) The applicant must ensure secure disposal of client's information including reports and supporting information after completion of engagement.

****

SECTION V – GUIDELINES FOR SUBMISSION OF INTEREST

1. Only applicants from Pakistan (National Competitive Bidding) are eligible to submit the response for the *Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform).*

2. Eligible Applicant(s) should submit **Expressions of Interest (EOI)** in English/Urdu language along with relevant complete details of their qualification and experience as requested under **Section III – Eligibility/Qualification Criteria.**

3. A pre-submission meeting will be held on **December 28, 2022** at **11:00 AM (PKT)** via Zoom. Applicants are encouraged to attend the meeting to gain clarity about the procurement process, scope, evaluation criteria or any other related aspects. Official minutes of the Pre-submission meeting shall be issued to all participating Applicants.

4. Applicants must provide unambiguous and clear information as per the above requirements and must provide only material that would be specific to the proposed services, and to avoid submitting generic promotional material.

5. If the EOI response consists of more than one volume, the applicant must number the volumes constituting the EOI and provide an indexed table of contents for each volume. All documents should be securely bound.

6. Any further information/clarification by the Client can be sought.

****

SECTION VI – LETTER OF SUBMISSION OF INTEREST

(On Firm's Letterhead)

Date: *dd-mm-yyyy*

IFP Title: *Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)*
Reference: *EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022*

To:

Director
General Services Department
SBP Banking Services Corporation
4th Floor BSC House, I. I. Chundrigar Road,
Karachi, Pakistan

We, the undersigned, apply to be shortlisted for the referenced EOI and declare that:

(a) **No reservations:** We have examined and have no reservations to the EOI Documents, including Addendum(s) No(s), issued in accordance with Instructions to Applicants **(ITA)***: [insert the number and issuing date of each addendum].*

(b) **No conflict of interest**: We have no conflict of interest.**;**

(c) **Eligibility**: We meet the eligibility requirements**,** we have not been suspended by the Procuring Agency based on execution of a Bid/Proposal Securing Declaration;

(d) **State-owned enterprise or institution:** [*select the appropriate option and delete the other*] [*We are not a state-owned enterprise or institution*] / [*We are a state-owned enterprise or institution*];

(e) **Not bound to accept:** We understand that you may cancel the Shortlisting/EOI process at any time without incurring any liability to the applicants. Only applicants who have been Shortlisted shall be entitled to participate further in the procurement proceedings

(f) **Bound to Submit Technical and Financial Proposals:** We understand that if we get shortlisted at the EOI stage, we will be bound to submit Technical and Financial Proposals.

(g) **True and correct:** All information, statements and description contained in the Application are in all respect true, correct and complete to the best of our knowledge and belief.

Signed: [insert signature(s) of an authorized representative(s) of the Applicant]

Name: [insert full name of the person signing the Application]

In the capacity of [insert capacity of the person signing the Application]

Duly authorized to sign the Application for and on behalf of: [insert full name of the Applicant

Address: _____

Dated: _____

SECTION VII – AUTHORIZATION FORM FOR APPLICANT'S REPRESENTATIVE

(On Firm's Letterhead)

Title: Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)
Date of Submission: **DD-MM-YYYY**
Reference No.: EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022

To,

The Director,
General Services Department,
SBP Banking Services Corporation,
4th Floor, BSC House, I.I. Chundrigar Road,
Karachi, Pakistan.

Dear Sir,

We, **M/s <Name of applicant>** , incorporated under <mention the relevant Act/ordinance/ regulation> having its registered office at **<complete business address>** do hereby nominate **Mr./Ms. <Complete Name>, <Designation>, Social Security Card/CNIC/Citizen Card <_____>** as our lawful representative to participate, correspond and fulfil all associated formalities of the subject submission on our behalf.

Official Seal & Signature of Applicant:	_____
Date:	_____

SECTION VIII – APPLICANT INFORMATION FORM

(On Firm's Letterhead)

Date: *dd-mm-yyyy*

IFP Title: *Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)*
Reference: *EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022*

Applicant's Name:	*[insert full name]*
Applicant's Country of Registration:	*[indicate country of Constitution]*
Applicant's year of Incorporation:	*[indicate the year of Constitution]*
Tax Registration Details	
Applicant's legal address:	*[insert street/ number/ town or city/ country]*
E-mail Address:	
Telephone/Mobile Number:	
Official Web Site:	
Applicant's Authorized Representative Information	**Name:** *[insert full name]* **Address:** *[insert street/ number/ town or city/ country]* **Telephone/Fax numbers:** *[insert telephone/fax numbers, including country and city codes]* **E-mail address:** *[indicate e-mail address]*
Attached are Copies of Original Documents of	• Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above, in accordance with **ITA 4.5.** • Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

SECTION IX – UNDERTAKING

(On Stamp Paper of Rs. 100/-)

Undertaking For Non-Blacklisting/Non-Debarment & Non-Sanctioning

Date: *dd-mm-yyyy*

IFP Title: *Engagement of a Firm to Conduct IT Security Review of Business Applications (DWH/DAP Platform)*
Reference: *EOI No. GSD (Proc. II) /OCISO-DAP Security Review/73477/2022*

Dear Concern,

I/We hereby confirm and declare that I/We, M/s ----------, has never been blacklisted/debarred under Rule 19 of PPR-2004 by any government/semi-government organization.

Detection of false declaration/statement at any stage of the entire application/Bidding Process / Currency of the Contract shall lead to disqualification and forfeiture of Bid Security or Performance Guarantee, as the case may be, and termination of the contract.

Seal & Signature of Firm:	_____
Date:	_____

****