Standard Bidding Document

Trade Based Money Laundering (TBML)
(Non-Consultancy Services)

National

Single Stage-Two Envelope

August 28, 2026

National Bank of Pakistan (Compliance Group),SVP
The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.
Phone: +92-213-890-2267, Email: teemar@nbp.com.pk

Table of Contents

PROCUREMENT NOTICE

PROCUREMENT OF NON-CONSULTANCY SERVICES

1. The **National Bank of Pakistan (Compliance Group)** has reserved Funds for the procurement planned for FY **2026-27**. The **National Bank of Pakistan (Compliance Group)** intends to apply part of the proceeds of this Fund to cover eligible payments under the contract for the "**Trade Based Money Laundering (TBML)**" with the reference of **"P97471"**

2. The **National Bank of Pakistan (Compliance Group)** invites Bids through **EPADS v2.0** from eligible Bidders registered on **EPADS v2.0** for provision of Non-Consultancy Services.

3. **Single Stage-Two Envelope** Procedure of Principal Method of Procurement (i.e. Open Competitive Bidding) will be used by adopting **Quality and Cost Based Selection (QCBS)**Technique for the subject procurement, in line with the Public Procurement Rules, 2004 and any Regulations, and Instructions issued by the Authority (from time to time).

4. All Bids must be accompanied by a Bid Security described in Bid Security Section in Bidding Document in the form of **Bank Guarantee** or Bid Securing Declaration on the prescribed format described.

5. E-Bidding documents, containing detailed terms & conditions, specifications and requirements etc. are available on **e-Pak Acquisition and Disposal System (EPADS)** at **https://epads.gov.pk/opportunities/federal/procurements/97471**.

6. The e-bids, prepared in accordance with the instructions in the e-Bidding documents, must be submitted through **EPADS v2.0** on or before **Thursday, September 24, 2026 11:00 AM**. E-bids will be opened on the same day at **Thursday, September 24, 2026 11:30 AM**. Manual submission of Bids shall not be entertained. Those vendors who have not yet registered on the new version of **EPADS v2.0,** may register themselves on **https://vendors.epads.gov.pk/**. A tutorial to explain the registration process is available at **https://www.youtube.com/watch?v=MNW6T38v7tc**

7. In terms of Rules 48 of Public Procurement Rules, 2004 Grievance Redressal Committee (GRC) is notified for the subject procurement and notification copy is available on the procuring agency's website and also available on **EPADS v2.0** as well as Authority's website at (**www.ppra.org.pk**).

National Bank of Pakistan (Compliance Group), SVP
The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor,
National Bank of Pakistan, Head Office Building, Karachi.
+92-213-890-2267
teemar@nbp.com.pk

Instructions to Bidders

A. Introduction

1. **Scope of Bids**

1.1. The Procuring Agency (PA), as indicated in the **Bids Data Sheet (BDS)** invites Bids through **EPADS v2.0** for the provision of Non-Consultancy Services for as specified in the BDS and **in Section Evaluation Criteria, Specifications & Schedule of Requirements**. The name, identification, and number of items/deliverables are provided in the **BDS**. **Single Stage-Two Envelope** procedure of the open competitive method shall be used. The successful Bidders will be expected to provide the services within the specified period and timeline(s) as stated in the **BDS**.

2. **Source of Funds**

2.1. Source of funds is referred in Clause-1 of Invitation for Bids.

3. **Fraudualent & Corrupt Practices**

3.1. As defined under Rule 2(1)(f) of the Public Procurement Rules, 2004.

4. **Eligible Bidders**

4.1. A bidder is eligible to participate in a procurement process if the bidder:

4.1.1. possesses or has access to the technical competence, financial resources, equipment and other physical facilities, personnel, managerial capability, experience and reputation necessary to complete the procurement contract;

4.1.2. has the legal capacity to enter into a procurement contract;

4.1.3. is not insolvent, in receivership, bankrupt or being wound up and its activities or affairs are not suspended or being administered under any Act, by a court or by a judicial officer;

4.1.4. is not the subject of legal proceedings for any of the matters mentioned in sub-rule (c);

4.1.5. has fulfilled or has made substantial arrangements satisfactory to the relevant authorities, to fulfil its obligations to pay taxes and social security (where applicable) other contributions of its employees; and

4.1.6. has not, or in the case of a company, its owners and beneficial owners, directors or officers have not, been convicted of a criminal offence related to:

4.1.6.1. its professional conduct; or

4.1.6.2. a bidder (or, in the case of a company, its key individuals such as owners, beneficial owners, directors, or officers) must not have engaged in any prohibited practice, such as fraud, corruption, collusion, or coercion, within the time period stated in the bidding documents, which can be up to three years before the start of the procurement process. Additionally, the bidder must not have been debarred (i.e., banned) from participating in public procurement processes in Pakistan or by any international organization or country. If they have, they are ineligible to participate in the current bidding.

4.2. The procuring agency may require a bidder participating in the procurement process to provide the prescribed documentary evidence or other information to satisfy itself that the bidder is qualified in accordance with the criteria in sub-clause (1).

4.3. A procuring agency shall set out in the bidding document all the criteria for qualification to be applied in accordance with sub-clause (1).

4.4. Except as permitted under the Ordinance, Rules and Regulations, the procuring agency shall not establish a criterion for eligibility of a bidder that:

4.4.1. discriminates against or among a bidder or against categories of bidders; or

4.4.2. is not required for the performance of the procurement contract; or

4.4.3. is not related to the avoidance or management of legal, reputational or economic risk to the procuring agency unless it is in the national interest to do so, and the criteria is set out in the bidding documents.

4.5. A procuring agency shall assess the eligibility of a bidder for participation in the procurement process against the criteria for qualification under sub-clause (1).

4.6. In the case of a joint venture, consortium, or association, all members shall be jointly and severely liable for the execution of the contract in accordance with the terms and conditions of the contract. The joint venture, consortium, or association shall nominate a lead member as nominated in the BDS,

4.7. who shall have the Authority to conduct all business for and on behalf of any and all the members of Joint venture, consortium, or association during the bidding process, and in case of award of contract, during the execution of the contract.

4.8. The appointment of the lead Member in the joint venture, consortium, or association shall be confirmed by submission of valid power of Attorney to the procuring agency.

4.9. Subject to the limits specified in the BDS, the procuring agency may allow bidders to participate in the form of a Joint Venture (JV). However, each party in the JV must individually meet the eligibility criteria specified in the BDS

4.10. No Bidder can be a sub-contractor while submitting a Bids individually or as a member of a joint venture in the same Bidding process.

5. **Qualification of the Bidder**

5.1. All Bidders shall provide in Section VI, Bid Forms, a preliminary description of the proposed work method and schedule, including drawings and charts, as necessary.

B. Bidding Documents

6. **Contents of Standard Bidding Document**

6.1. The Services required, bidding procedure, and terms and conditions of the contract are prescribed in the bidding document. In addition to the Invitation for Bids, the bidding document which should be read in conjunction with any addendum issued by the Procuring Agency include:

Section I -Invitation to Bid
Section II Instructions to Bidders (ITB)
Section III Bid Data Sheet (BDS)
Section IV Eligible Countries
Section V Evaluation Criteria, Specifications, Schedule of Requirements, and Technical Specifications.
Section VI Bidding Forms
Section VII Fraudaulent & Corrupt Practices
Section VIII – Material & Non-material deviation
Section IX General Conditions of Contract (GCC)
Section X Special Conditions of Contract (SCC)
Section XI Contract Forms

6.2. The Bidder is expected to examine all instructions, requirements, forms, terms and specifications in the bidding documents. Failure to furnish all the information required in the bidding document will be at the Service provider’s risk and may result in the rejection of his bids.

7. **Clarifications**

7.1. Clarifications of the bidding documents may be requested in writing through EPADS v2.0 by any bidder up to three days prior to the deadline for the submission of bids.

The procuring agency shall respond promptly and in writing to any request by a bidder for clarification of the bidding documents and, in any event, no later than two days prior to the deadline for the submission of bids or proposals.

Responses to requests for clarification shall be communicated simultaneously and in writing to all bidders participating in the procurement proceedings.

No bidder shall be allowed to alter or modify his bid after the bids have been opened however, the procuring agency may seek and accept clarification to the bid that do not change the substance of the bid, through EPADS v2.0.

7.2. Procuring Agency's response will be uploaded on the EPADS v2.0, including a description of the inquiry.

7.3. Should the Procuring Agency deem it necessary to amend the bidding document as a result of a clarification, it shall do so following the procedure under **ITB 1.1.**

7.4. If indicated **in the BDS**, the bidder’s designated representative is invited at the bidder’s cost to attend a pre-bid meeting at the place, date and time mentioned **in the BDS**. During this pre-bid meeting, prospective bidder(s) may request clarification(s) regarding the schedule of requirements, the Evaluation Criteria or any other aspects of the bidding document.

7.5. Minutes of the pre-bid meeting, if applicable, including the text of the questions asked by bidders, and the responses given, together with any responses prepared after the meeting will be uploaded on EPADS v2.0. Any modification to the bidding document that may become necessary as a result of the pre-bid meeting shall be made by the Procuring Agency exclusively through the use of an Addendum.

7.6. To assist in the examination, evaluation and comparison of Bids of the Bidders, the Procuring Agency may, ask any Bidder for a clarification of its bid including breakdown of prices, through EPADS v2.0. Any clarification submitted by a bidder that is not in response to a request by the Procuring Agency shall not be considered.
No change in the prices or substance of the bid shall be sought, offered, or permitted.
The alteration or modification in the bid which in any way affect the following parameters will be considered as a change in the substance of a

bid:

7.6.1. evaluation & qualification criteria;

7.6.2. required scope of work or specifications;

7.6.3. all securities requirements;

7.6.4. tax requirements;

7.6.5. terms and conditions of bidding documents; and

7.6.6. change in the ranking of the bidders.

From the time of bid(s) opening to the time of contract award, if any bidder wishes to contact the procuring agency on any matter related to the bid, it should do so in writing or through electronic form that provides record of the content of communication.

8. **Amendment of Bidding documents**

8.1. Before the deadline for submission of bids, the procuring agency for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder or pre-bid meeting may modify the bidding documents by issuing addendum.

8.2. Any addendum issued including the notice of any extension of the deadline shall be part of the bidding document and shall be uploaded on EPADS v2.0 as well as Authority's website. The procuring agency shall promptly publish the addendum at the procuring agency's website indicated in the **BDS**:

Provided that the bidder who had either already submitted his bid, shall have the right to withdraw his already submitted bid and submit the revised bid, prior to the original or extended bid submission deadline.

8.3. To give prospective bidders reasonable time in which to take an addendum/corrigendum into account in preparing their bids, the Procuring Agency may, at its discretion, extend the deadline for the submission of bids:

Provided that the Procuring Agency shall extend the deadline for submission of bids, if such an addendum is issued within last three (03) days of the bid submission deadline.

C. Preparation of Bids

9. Documents Constituting the Bids

9.1. The bids prepared by the bidders shall constitute the following components: -

9.1.1. Forms of bid and Bid Prices completed in accordance with ITB BDS, GCC and SCC;

9.1.2. Documentary evidence established in accordance with BDS that services to be provided by the bidder are eligible services, and conform to the bidding documents;

9.1.3. Documentary evidence established in accordance with BDS that the bidder is eligible and/or qualified for the subject bidding process;

9.1.4. Documentary evidence established, that the bidder has been authorized to provide the services;

9.1.5. Bid security or Bids Securing Declaration furnished in accordance with BDS; and

9.1.6. Any other document required in the BDS.

10. **Documents Establishing Eligibility of the Services and Conformity to bidding documents**

10.1. To establish the conformity of the Non-Consulting Services to the Bidding document, the bidder shall furnish as part of its bid the documentary evidence that services provided conform to the requirements.

10.2. Standards for the provision of the Non-Consulting Services are intended to be descriptive only and not restrictive.

11. **Documents Establishing Eligibility and Qualification of the Bidder**

11.1. Pursuant to BDS, the bidder shall furnish, as part of itsbid, all those documents establishing the bidder's eligibility to participate in the bidding process and/or its qualification to perform the contract if its bid is accepted.

11.2. The documentary evidence of the bidder's eligibility to bids shall establish to the satisfaction of the procuring agency that the bidder, at the time of submission of its bid, is from an eligible country as defined in Section-IV titled as "Eligible Countries".

11.3. The documentary evidence of the bidder's qualifications to perform the contract if its bid is accepted shall establish to the satisfaction of procuring agency that:

11.3.1. the bidder has the financial, technical, and supply/production capability necessary to perform the Contract, meets the qualification criteria specified in BDS.

11.3.2. that the bidder meets the qualification criteria listed in the Bids Data Sheet.

12. **Form of Bid**

12.1. **The bidder shall fill the Form of Bid furnished in the bidding documents. The Bid Forms must be completed without any alterations to its format and no substitute shall be accepted.**

13. **Bids Prices**

13.1. The Bids Prices quoted by the bidder in the Forms of Bid and in the price schedule shall conform to the requirements specified or exclusively mentioned hereafter in the bidding document.

13.2. All items in the Schedule of Requirements must be listed and priced separately in the Price Schedules. If a Price Schedule shows items listed but not priced and neither explicitly mentioned, their prices shall be construed to be included in the prices of other items.

13.3. The Bid price to be quoted in the Forms of Bid shall be the total price of the bid, excluding any discounts offered.

13.4. The bidder shall indicate on the appropriate Price Schedule, the unit prices (where applicable) and total bid price of the services, it proposes to provide under the contract.

13.5. Prices quoted by the bidder shall be fixed during the currency of the contract and not subject to variation on any account. A bid submitted with an adjustable price will be treated as non-responsive and shall be rejected, unless otherwise price adjustment is permissible under Conditions of the Contract. (May be reviewed)

14. **Price Adjustment**

14.1. Price adjustment shall not be applicable.

14.2. Procuring agency may increase the remuneration of the human resources involved in non-consultancy services on annual basis as per agreement.

14.3. **Procuring agency shall incorporate the provisions to allow wage rate in compliance with Federal Government's minimum wage notification, subject to the applicability in that case.**

15. **Bids Currencies**

15.1. Prices shall be quoted in Pakistani Rupees unless otherwise specified in the BDS.

16. **Bid Validity Period**

16.1. Bid(s) shall remain valid for the period specified in the BDS after the bid submission deadline prescribed by the Procuring Agency. A Bid valid for a shorter period shall be rejected by the Procuring Agency as non-responsive. The period of bid validity will be determined from the complementary bid securing instrument i.e. the expiry period of bid security or bid securing declaration as the case may be.

17. **Bid Security or Bid Securing Declaration**

17.1. Unless otherwise specified in the BDS, the bidder shall furnish as part of its bid, in the amount and currency specified in the BDS or Bid Securing Declaration on the format provided in Section VI (Bid Forms) The scanned copy of the Bids Security shall be uploaded in the EPADS v2.0 while submitting bid, whereas the original forms of Bid Security shall be submitted to the procuring agency before the bid submission deadline. The bidder who failed to submit the original bid security before the submission deadline shall be disqualified straightaway.

17.2. The Bid Security or Bid Securing Declaration is required to protect the Procuring Agency against the risk of Bidder’s conduct which would warrant the security’s forfeiture.

17.3. The Bid Security shall be payable promptly upon written demand by the Procuring Agency in case any of the conditions listed in BDS, GCC and SCC are invoked.

17.4. Unsuccessful Bidders’ Bid Security will be discharged or returned as promptly as possible after the award of contract, however in no case later than thirty (30) days after the expiration of the period of Bid Validity prescribed by the Procuring Agency. The Procuring Agency shall make no claim to the amount of the Bid Security, and shall promptly return the Bid Security document, whichever of the following that occurs earliest:

17.4.1. the expiry of the Bid Security;

17.4.2. the entry into force of a procurement contract and the provision of a Performance Guarantee, for the performance of the contract if such a guarantee, is required by the bidding document;

17.4.3. the rejection by the Procuring Agency of all Bids;

17.4.4. the withdrawal of the Bid prior to the deadline for the submission of bids, unless the bidding document stipulate that no such withdrawal is permitted.

17.5. The Bid Security may be forfeited or the Bid Securing Declaration executed:

17.5.1. if a bidder:

17.5.1.1. withdraws its bid during the period of bid validity as specified by the Procuring Agency, and referred by the bidder in the Forms of Bid, except as provided for in the ITBs; or

17.5.1.2. does not accept the correction of errors, or

17.5.2. in the case of a successful bidder fails:

17.5.2.1. **to sign the contract in accordance with SCC; or**

17.5.2.2. **to furnish Performance Guarantee in accordance with BDS and SCC.**

17.6. **The bid security shall be valid for a period specified in BDS. Bids with shorter bid security validity period shall be rejected straight away.**

18. **Alternative Bids by Bidders**

18.1. Alternatives will not be considered, unless specifically allowed for in the BDS.

18.2. When alternative times for completion are explicitly invited, a statement to that effect will be included in the BDS and the method of evaluating different time schedules will be described in Evaluation and Qualification Criteria.

19. **Withdrawal, Substitution, and Modification of Bids**

19.1. Before Bids submission deadline, any bidder may withdraw, substitute, or modify his bid after it has been submitted.

20. **Format and Signing of Bids**

20.1. The bidder shall prepare and submit his bid with due diligence after carefully reading all the terms and conditions before submission through

EPADS v2.0.

20.2. Any interlineations, erasures, or overwriting shall be valid only if they are signed by the person(s) signing the forms of bid.

D. Submission of Bids

21. **Submission of Bids through EPADS v2.0 before Dead deadline**

21.1. The Technical and Financial Bids as the case may be, shall be submitted in the due portion of the EPADS v2.0, before bid submission deadline. The bid submission option shall be automatically disabled once the deadline is over.

21.2. The Procuring Agency may, under exceptional circumstances and at its discretion, extend the deadline for the submission of bids by amending the Bidding Documents. In such a case, all rights and obligations of the Procuring Agency and the Bidders that were previously subject to the original deadline shall thereafter be subject to the revised deadline.

E. Opening and Evaluation of Bids

22. **Opening & Evaluation of Bids by the Procurement Cell/Evaluation Committee**

22.1. The Procuring Agencies to constitute odd number Bid Evaluation Committee for the purpose of bid opening and evaluation of all procurements. As per Rules 29 & 30 of Public Procurement Rules, 2004,
The Procuring Agencyis required to establish a Procurement Cell/Evaluation Committee which shall Evaluate the Bids inaccordance with the evaluation criteria, terms and conditions given in the bidding documents.

23. **Opening of Bids**

23.1. The Bid Evaluation Committee of the Procuring Agency will open all bids through EPADS, in the presence of bidders' or their representatives who

choose to attend, and other parties with a legitimate interest in the bid proceedings at the place, on the date and at the time, specified in the **BDS**. The Bidders' representatives present shall sign attendance sheet as proof of their attendance.

23.2. The bids shall be opened one at a time, and the following read out and recorded: (a) the name of the bidder; (c) the presence of a bid security, if required; and (d) any other details as the procuring agency may consider appropriate.

23.3. No bid will be rejected at the time of bid opening except for bids whose bid security has not been provided to the procuring agency before submission deadline**.**

23.4. The procuring agency shall prepare minutes of the bid opening. The record of the bid opening shall include, as a minimum: the name of the bidder and the bid price, if applicable.

24. **Confidentiality**

24.1. Information relating to the examination, clarification, evaluation and comparison of bids and recommendation of contract award shall not be disclosed to bidders or any other person(s) not officially concerned with such process, until the time of the announcement of the respective evaluation report.

24.2. Any effort by a bidder to influence the procuring agency processing of bids or award decision may result in the rejection of his bid.

25. **Preliminary Examination of Bids**

25.1. Prior to the detailed evaluation of bids, the procuring agency will determine whether each bid:

25.1.1. meets the eligibility criteria defined in **BDS**;

25.1.2. has been prepared as per the format and contents defined by the procuring agency in the bidding document;

25.1.3. is accompanied by the required securities; and

25.1.4. is substantially responsive to the requirements of the bidding document.

25.2. The procuring agency will confirm that the documents and information specified under **BDS, GCC and SCC** have been provided in the bids. If any of these documents or information is missing, or is not provided in accordance with the Instructions to Bidders, the bids shall be rejected.

25.3. If a bid is not substantially responsive, it will be rejected by the procuring agency and may not subsequently be evaluated for complete technical responsiveness.

26. **Examination of Terms and Conditions, Technical Evaluation**

26.1. The procuring agency shall evaluate the technical aspects of the bids submitted in accordance with **BDS,** to confirm that all requirements specified in **Evaluation Criteria, Technical Specifications and Schedule of Requirements**, prescribed inthe bidding document have been met without material deviation or reservation.

26.2. If after the examination of the terms and conditions and the technical evaluation, the procuring agency determines that the bid is not substantially responsive in accordance with BDS**,** it shall reject the bids.

27. **Correction of Errors**

27.1. Bids determined to be substantially responsive will be checked for any arithmetic errors. Errors will be corrected as follows: -

27.1.1. if there is a discrepancy between unit prices and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected, unless in the opinion of the procuring agency there is an obvious misplacement of the decimal point in the unit price, in which the total price as quoted shall govern and the unit price shall be corrected;

27.1.2. if there is an error in a total corresponding to the addition or subtraction of sub-totals, the sub-totals shall prevail and the total shall be corrected; and

27.1.3. where there is a discrepancy between the amounts in figures and in words, the amount in words will govern.

27.1.4. Where there is discrepancy between grand total of price schedule and amount mentioned on the Forms of bid, the amount referred in Price Schedule shall be treated as correct subject to elimination of other errors.

27.2. The amount stated in the bid will be adjusted by the procuring agency in accordance with the above procedure for the correction of errors and, with the concurrence of the bidder that shall be considered as binding upon the bidder. If the Bidder does not accept the corrected amount, his bid will then be rejected, and the Bid Security may be forfeited or the Bid Securing Declaration may be executed.

28. **Conversion to Single Currency**

28.1. As per Rule 30 of Public Procurement Rules, 2004.

29. **Evaluation of Bids**

29.1. The procuring agency shall evaluate bids in accordance with Rule 30 of Public Procurement Rules, 2004 and compare only those bids determined to be substantially responsive.

29.2. In evaluating the Technical Bids of each Bidder, the Procuring Agency shall apply the evaluation criteria and methodologies specified in the Bid Data Sheet (BDS) and in accordance with the Statement of Requirements and Technical Specifications. No other evaluation criteria or methodologies shall be permitted.

29.3. In case of tie of bids, the bidders shall be provided an opportunity to offer their best and final monetary offer through EPADS. However, in no case the rates shall be higher than the original financial bids.

29.4. The Procuring agency evaluation of a bid will take into account:

29.4.1. the bid price, excluding provisional sums and the provision, if any, for contingencies in the summary bill of quantities, but including day work items, where priced competitively;

29.4.2. price adjustment for correction of arithmetic errors in accordance with **ITB 6;**

29.5. converting the amount resulting from applying (a) and (b) above, if relevant, to a single currency in accordance with **ITB 7**;

29.6. The estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be taken into account in bid evaluation.

29.7. If these bidding documents allow bidders to quote separate prices for different lots, and the award to a successful bidder of multiple lots, the methodology of evaluation to determine the lowest evaluated lot combinations in the Form of Bid, is specified in the **BDS.**

30. **Determination of Most Advantageous Bids**

30.1. Selection technique will be adopted for determining the Successful Bid in accordance with the criteria referred in the **BDS** or prescribed in the separate section titled as Evaluation Criteria.

31. **Abnormally Low Financial Bids**

31.1. Procuring agency may reject a bid if it has determined that the price, in combination with other constituent elements of the bid, is abnormally low in relation to the subject matter of the procurement, such that it raises material concerns on the part of the procuring agency, as to the ability of the bidder to perform the procurement contract satisfactorily for the offered price.

A procuring agency shall not reject a bid as abnormally low under sub-clause (1) above unless the procuring agency –

31.1.1. requested in writing through EPADS from the bidder a written clarification of his bid, including a detailed price analysis of his bid price in relation to the subject matter of the procurement contract, scope, methodology, schedule, allocation of risks and responsibilities and any other requirements of the bidding document; and

31.1.2. having taken account, the information provided by the bidder in response to a request under paragraph (a) and the information included in the bid, the procuring agency determines that the bidder has failed to demonstrate its ability to perform the procurement contract satisfactorily for the offered price.

The procuring agency shall promptly communicate to the bidder concerned its decision to reject the bid, including the reasons for the decision.

32. **Rejection of Bids**

32.1. As per Rule 33 of the Public Procurement Rules, 2004

33. **Single Responsive Bid**

33.1. The procuring agency may consider single responsive bid subject to underlying conditions of Rule 38(b) of the Public Procurement Rules, 2004.

34. **Arbitration**

34.1. As per Rule 49 of Public Procurement Rules, 2004.

F. Award of Contract

43. **Criteria of Award**

43.1. The procuring agency will award the Contract to the bidder whose bid has been determined to be substantially responsive to the bidding document and who has been declared as most advantageous Bid.

44. **Procuring Agency's Right to reject All Bids**

44.1. The procuring agency reserves the right to reject all the Bids and to annul the procurement process at any time prior to acceptance of the bid(s), without thereby incurring any liability to the affected bidder(s).

44.2. Notice of the rejection of all bids shall be given promptly to all bidders that have submitted the bids. The procuring agency shall upon request communicate to any bidder the grounds for the rejection of his bid, but is not required to justify those grounds.

45. **Notification of Award**

45.1. Prior to the award of contract, the procuring agency shall issue a Final Evaluation Report giving justification for acceptance or rejection of the bids.

45.2. Bidder whose bid has been accepted, will be notified for the award by the Procuring Agency prior to expiration of the Bid Validity period through EPADS. The Letter of Acceptance will state the sum that the procuring agency will pay the successful bidder in consideration for the execution of the scope of works as prescribed by the Contract (hereinafter and in the Contract called the "Contract Price).

45.3. The notification of award will constitute the formation of the Contract, subject to the condition that bidder furnish the Performance Guarantee and signing of the contract.

46. **Signing of Contract**

46.1. Promptly after notification of award, Procuring Agency shall send the successful bidder the draft agreement, incorporating all terms and conditions as agreed by the parties to the contract. The successful bidder and the procuring agency shall sign the contract.

47. **Performance Guarantee**

47.1. After the receipt of the Letter of Acceptance, the successful bidder, within the specified time, shall deliver to the Procuring Agency a Performance Guarantee in the amount and in the form stipulated in the **BDS**

and SCC, denominated in the type and proportions of currencies in the Letter of Acceptance and in accordance with the Conditions of Contract.

47.2. Failure of the successful bidder to comply with the requirement of **BDS, SCC and GCC** shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the procuring agency may make the award to the next ranked bidder or call for new bids.

48. **Corrupt & Fraudulent Practices**

48.1. Procuring Agencies (including beneficiaries of Government funded projects and procurement) as well as Bidders/Contractors under Government financed contracts, observe the highest standard of ethics during the procurement and execution of such contracts, and will avoid to engage in any corrupt and fraudulent practices.

G. Grievance Redressal & Complaint Review Mechanism

53. **Constitution of Grievance Redressal**

53.1. Procuring agency shall constitute a Grievance Redressal Committee (GRC) comprising of an odd number of persons with proper power and authorization to address the complaint. The GRC shall not have any of the members of Procurement Evaluation Committee.

54. **GRC Procedure**

54.1. Any aggrieved party or bidder as the case may be, may file grievance in accordance with Rule 48 of the Public Procurement Rules, 2004 and Redressal of Grievance Regulations, 2022

H. Blacklisting/ Debarment

55. **Procedure for Blacklisting/Debarment**

55.1. The procuring agency may initiate blacklisting proceedings against contractor/supplier in accordance with Rule-19 of the Public Procurement

Rules, 2004 , Mechanism for Blacklisting, Debarment Regulations, 2024 and Regulation on “procedure for filling and disposal of review petition under rule-19(3) of the Public Procurement Rules, 2004.

Bid Data Sheet

Bids Data Sheet (BDS)

The following specific data for the procurement of Non-Consultancy Services to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

BDS Clause Number
ITB Number

Amendments of, and Supplements to, Clauses in the Instruction to Bidders

A. Introduction

BDS Clause Number 1

Name of Procuring Agency: **National Bank of Pakistan (Compliance Group)**

The subject of procurement is: **Trade Based Money Laundering (TBML)**

Expected commencement date: **Wednesday, March 31, 2027**

BDS Clause Number 2

Financial year for the operations of the Procuring Agency: **2026-27**

Name and identification number of the Contract: **P97471**

BDS Clause Number 3

JV/Consortium or Association Allowed: **No**
Number of JV/Consortium Members: **Nil**

B. Bidding Documents

BDS Clause Number 4

The Bidders may seek clarifications through **EPADS v2.0**: Clarification Date: Tuesday, September 15, 2026

BDS Clause Number 5

Any addendum, in case issued, shall be published on **National Bank of Pakistan (Compliance Group)** website and on **EPADS v2.0**.

BDS Clause Number 6

List of documents required along with the bid:

1. All required documents as mentioned in Eligibility Criteria & Techincal Evaluation.

BDS Clause Number 7

The qualification criteria to establish the supply / production capability of the bidder.

see Eligibility Criteria

BDS Clause Number 8

Services and Their related documents:
See section Required Services and Scope of Work

BDS Clause Number 9

Price schedule will be provided according to the format defined and acquired.
see section price schedule.

BDS Clause Number 10

Specifications:

see section of specifications.

C. Preparation of Bids

BDS Clause Number 11

The price shall be **Fixed**.

BDS Clause Number 12

Currency of the Bids shall be : **PKR**

BDS Clause Number 13

The Bids/Bid Validity period shall be: **180 Days**

BDS Clause Number 14

The amount of Bid Security shall be as defined in Bid Security Section for items and lots given in **BDS 6**
The Bid Security shall be in the form of: **Bank Guarantee**

BDS Clause Number 15

The Bids security shall be valid for twenty-eight (28) days beyond the expiry of the Bids validity period specified in the bidding documents, for example the bid validity is 90 days so the bid security shall be valid for 90+28 = 118 days.

BDS Clause Number 16

Alternative Bids to the requirements of the bidding documents will not be permitted.

D. Submission of Bids

BDS Clause Number 17

Bid shall be submitted online on EPADS v2.0 whereas hard copy of the bid security should be submitted to the following;

The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.

Bids that are not submitted on EPADS v2.0 shall be disqualified.

The deadline for Bids submission is: **Thursday, September 24, 2026 11:00 AM**

E. Opening and Evaluation of Bids

BDS Clause Number 18

The Bids opening shall take place on **EPADS v2.0**.

Day *:* ***Thursday***

Date: ***Thursday, September 24, 2026***

Time *:* ***11:30 AM***

BDS Clause Number 19

Selection technique adopted will be: **Quality and Cost Based Selection (QCBS)**
see Evaluation Criteria

F. Award of Contract

BDS Clause Number 20

The Performance guarantee shall: **10.00%**.

The Performance Guarantee shall be acceptable in the form of: **Banker's Cheque, Bank Guarantee**

21.

51.1

Arbitrator shall be appointed by mutual consent of the both parties.

G. Review of Procurement Decisions

BDS Clause Number 22

Grievence against this procurement shall be submitted online on EPADS v2.0.

Eligibility Criteria

Bidder's Type	Required Registration
Company (Private Limited)	NADRA CITIZENSHIP (CNIC/NICOP) FBR (NTN) FBR (GSTN) SECP

Eligibility Criteria	Document
Bidders must have a documented track of at least two (2) live implementations locally or globally of “Trade Based Money Laundering System” and providing Maintenance and Technical support as the direct authorized agent / dealer / partner of the manufacturer in Pakistan. Bidder must provide Reference Letters / Purchase / Work Orders from the customers where the solution is deployed and last implementation details.	Yes
The bidders must have verifiable presence/support/branch office in Pakistan.	Yes
Bidder must provide audited Profit & Loss (Income Statement) showing Sale volume of company of at least Rs.50 Million in each last 3 years.	Yes
Bidder must provide an undertaking on non-judicial stamp paper of 500 Rupees stating that "the bidder's company is not blacklisted by any Government entity in Pakistan for unsatisfactory past performance, corrupt, fraudulent or any other unethical business practices and also not involved in any kind of lawsuits either current or pending." (The undertaking on legal paper provided by the bidder must cover all points in the statement mentioned above).	Yes

Bidder must provide 03(three) CV's/Profile of their proposed implementation and configuration team which should be employees of the company since last one year and must have relevant experience for proposed solution	Yes
Bidder must have Direct Partnership with the principal supplier and also must provide "Manufacturer Authorization Form / Authorized Partner / Distribution Certificate" from principal supplier as per the requirements (guarantee, warranty and maintenance etc.).	Yes
Bidder must provide undertaking that the proposed solution is an international or national level solution. The bidder must also confirm therein that he is content specialist for the proposed solution.	Yes
Bidder must be CMMI Level 3 or above compliant or have other equivalent certifications.	No
Bidder must provide Solution architecture diagram and technical requirement of proposed solution.	Yes
SRB (Sindh revenue Board Certificate)	Yes

Evaluation Criteria

Quality and Cost Based Selection (QCBS)

Weightage

Technical Evaluation %	Financial Evaluation %
70	30

Technical Marks	100
Passing Marks	**80**
General Requirements	
"Vendor will perform business analysis and customize the software in order to capture relevant requirements and all details necessary for the design of the required solution as per State Bank of Pakistan Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing issued in 2019, SBP Framework for TBML is here under: Including but not limited to the following: · Implementation of required modules with all features and controls to meet regulatory requirement and minimum human interaction and intervention. · The vendor shall provide plan on training, tutoring, including comprehensive training contents and share all mandatory material to business users and IT Staff including but not limited to provisioning of user manual and administrative guide. · Timely solution to the problem through on-site visit. (Quantitative)(Doc Required)	1
The Vendor will ensure smooth implementation of Trade Based Money Laundering System so that the day-to-day activities of Trade Operations, Compliance and Risk Management function will continue uninterrupted. (Quantitative)(Doc Required)	1

"Vendor shall implement the following module for NBP TBML system : 1. Price Due Diligence 2. Vessel Tracking 3. Container Tracking 4. Dual Use Goods 5. TBML Scenarios 6. Trade Documents Validation 7. MIS & Dashboards 8. Integration with Bank Systems Each Module should have “Help Option” display for each item with description. Video Tutorial/training material tab on each module." (Quantitative)(Doc Required)	1
System must be capable of providing reports for audit trail with time and date stamp (Quantitative)(Doc Required)	1
"a) System must be complied with SSDLC checklist (refer: Annexure I) provided by bank's information Security Division(ISD) for Bidder Qualification and Technical Requirements. Bidder also need to complied any new requirement by SBP or NBP ISD during implementation/Go-Live. b) In case of cloud based solution, compliance with SBP regulations should be mandatory. (refer: Annexure II)" (Quantitative)(Doc Required)	1
Upon selection of bidder, Functional specification document (FSD) with complete architecture diagram with respect to NBP environment (including communication protocol, authentication mechanism, integration with other components like TI, etc.) should be provided before deployment phase. (Quantitative)(Doc Required)	1
Regulation Assessment, Maintenance & Updation	
The vendor shall ensure that the system shall have a process to identify and upgrade the system as per new/ evolving regulatory requirements without additional cost. (Quantitative)(Doc Required)	1
Price Due Diligence	
The system shall be capable of evaluating the deviation in pricing between the amount/ value of underline goods/ commodity input in the system based on shipping documents and the prices available on multiple reliable resources which includes but not limited to FBR, PSW, WEBOC, OGRA, Platts of all regions, shipping line data, TDAP, websites, historical appraisement etc. on real time basis in terms of percentage and absolute value as defined in the SBP Framework on TBML issued in 2019. (Quantitative)(Doc Required)	1

"The system shall maintain and update the following list - List of goods which are exempt from import-related duties. - list of goods which are subject to over 25% import-related duties This data should be used by system in evaluating price variance. " (Quantitative)(Doc Required)	1
"a) The system shall have capability to validate HS code , unit of measure & custom duty against the product description b) The system shall be capable to give alert if the deviation in the price is more than given threshold as per bank policy and subject to change whenever required. c) The system shall be capable to evaluate the deviation all the components of price including but not limited to Unit Price (FoB), Freight & other components like premium etc. Each product has different components of pricing which should be catered accordingly." (Quantitative)(Doc Required)	1
The system shall be capable to generated report with complete details with Time and date stamp for audit trail purpose. (Quantitative)(Doc Required)	1
Vessel Tracking	
The system shall be capable to provide vessel Information which includes but not limited to Name. AIS Name, IMO number, Country, Country ISO, Type, Year Built, Weigh & Size, Home port, European Number of Identification etc. (Quantitative)(Doc Required)	1
The system shall be capable to provide vessel position on real time basis and tracking record which includes but not limited to Last Position, Last Position Date, Region, Nearest Port and its distance, Departure Port, Destination Port, Actual time of Departure, estimated time of arrival, details of instance in case vessel had touched or come close to any sanction port/ country/ vessel, details of instance in case vessel had switched off transponder in past etc. (Quantitative)(Doc Required)	1
"a) The system shall be capable to provide vessel Ownership which includes but not limited to Cover Flag, Owner, Manager, Operator, Technical Manager, insurer etc. b) The system shall be capable to verify the Bill of Lading" (Quantitative)(Doc Required)	1
The system shall be capable to generate the report with date and time stamp for audit trail. (Quantitative)(Doc Required)	1

Container Tracking	
"a) The system shall be capable to provide container information which includes but not limited to type, number, status, sealine name, ISO Code, AT, Transshipment, Sanction country, departure port, Arrival port, Discharge port and IMO, Vessel Flag of vessel in which it is placed etc. b) The system shall be capable to Track containers events like Empty to shipper, arrival at first port of loading, loading and discharge at transshipment (T/S) ports, vessel departure and arrival etc. " (Quantitative)(Doc Required)	1
The system shall be capable to search container through various information like Container number, booking number and its tracking and navigation details should be provided by system. (Quantitative)(Doc Required)	1
The system shall be capable to provide mapping on real time basis and historical tracking record (Quantitative)(Doc Required)	1
Dual Use Goods	
The system shall be capable to identify whether a specific product is subject to import and export control regulation. (Quantitative)(Doc Required)	1
The system shall be capable to identify/ detect the underline Good as Dual Use Good by using information like Product Name, CAS number, HS Code, category, sub-category, serial number etc. (Quantitative)(Doc Required)	1
The system shall be capable to update the list of Dual Use Goods as per latest regulatory changes. (Quantitative)(Doc Required)	1
"The system shall be capable to over complete range of Dual Use Goods by using different list including but not limited to following; - Sec Div - Wassenaar - United States Commerce Control List - United Kingdom Strategic Control List" (Quantitative)(Doc Required)	1
TBML Scenarios	

The system shall be capable to detect Red Flags in the transactions on Pre-check and Post-Check basis. (Quantitative) (Doc Required)	1
"a) The system shall have comprehensive list of TBML Red Flags including but not limited to Red Flags given by SBP & FMU in their Regulations respectively. b) The system shall have option of Case Management of Alerts." (Quantitative)(Doc Required)	1
The system shall have ability to update the Red Flags are the latest guideline, regulations and industry practice. (Quantitative)(Doc Required)	1
The system shall have capability to maintain historical records of Red Flags, alerts, scenarios, cases and system changes. (Quantitative)(Doc Required)	1
Trade Documents Validation	
The system shall be capable to match GD declared value with the payment against import/ export bills and generate alert in case of deviation. (Quantitative)(Doc Required)	1
"a) The system shall be capable to detect deviations between GD declared v/s assessed value b) The system shall be capable to detect deviation between FIs details and GDs. " (Quantitative)(Doc Required)	1
The system shall be capable to detect duplication of Invoices, Goods Declaration, Transport Documents already used (Quantitative)(Doc Required)	1
MIS & Dashboards	
The system shall be capable to generated meaningful MIS by using available information to give end to end view of trade portfolio and audit trail. (Quantitative)(Doc Required)	1
The system shall be capable to formulate different Dashboards to analyze trade data, monitor compliance and extract valuable insight for historical analysis and status updates. (Quantitative)(Doc Required)	1

The system shall be capable to generate reports of non-performance and overdue status of import payments and export receipts respectively to meet regulatory requirements. (Quantitative)(Doc Required)	1
Integration with Bank Systems	
The system shall be capable to integrate with existing bank system including but not limited to Trade Application (TI+), Account Opening System (AOS), Core Banking System (CBA) for smooth data exchange and process automation. (Quantitative)(Doc Required)	1
The system shall restrict duplicate data entry by automating data capture and synchronization across systems through real time connectivity. (Quantitative)(Doc Required)	1
Access and Control	
The system shall be capable to implement robust controls to ensure security and confidentiality (Quantitative)(Doc Required)	1
The system shall be capable to define user roles, assign permissions as per department/role. (Quantitative)(Doc Required)	1
System shall not use built-in super admin ID to run systems operations for routine tasks. (Quantitative)(Doc Required)	1
System should be capable to assign limited administrative authority to named authorized application administrators. (Quantitative)(Doc Required)	1
System shall be capable of integration with the SIEM solution for information security at NBP. (Quantitative)(Doc Required)	1
Performance	
Ability to perform at or above specifications. Fast as possible with acceptable performance in regions with poor internet performance. (Quantitative)(Doc Required)	1
System must support multiple users. (Minimum 30 concurrent users) (Quantitative)(Doc Required)	1

Support	
Support through multiple mediums. (E.g. Email, fax, telephone, chat, helpdesk portal with ticketing system, etc.) Bidder should have 24x7x365 Corporate Helpline availability for reporting and resolution of all kinds of issues and escalations via including Phone Support, Email Support or Online customer portal to access support tickets for escalation and resolution (Quantitative)(Doc Required)	1
Bidder must provide complaint reporting and escalation matrix and/or software solution for NBP to report any issue / complaint and its rectification / resolution in the proposed solution. (Quantitative)(Doc Required)	1
Onsite or Virtual Support within Pakistan should be available. (Quantitative)(Doc Required)	1
Implementation	
Bidder before the start of implementation must provide hardware and software requirement , the entire installation process / implementation guidelines to NBP, including the installations related to application / database / web server etc., in conjunction with all other suppliers and contractors. (Quantitative)(Doc Required)	1
"a) Bidder must provide relevant examples/supported by rationale, of previously implemented in similar projects. Examples may include but not limited to strategy and execution plan, production of any digital content, production of any print content, distribution mechanism. b) System must support text editor, embed external resources, multimedia integration including video, audio and presentation files." (Quantitative)(Doc Required)	1
Bidder is required to provide the Proof of Concept (POC) of the proposed solution along with the presentation / solution screenshots with the proposal. Presentations / Demo session will be scheduled as per NBP requirements. (Quantitative) (Doc Required)	1
Testing	

"Bidder should provide the performance benchmark / metrics of the proposed solution. Note: The bidder would also develop and provide a testing methodology for the provided performance benchmark/metrics of the proposed solution, in coordination with NBP, after being awarded the contract. NBP will perform testing (which may not be limited to single test cycle) of complete solution after its deployment and any gaps found therein would be fixed by the bidder without any additional cost." (Quantitative)(Doc Required)	1
Issues / bugs reporting, tracking and resolution tools must be provided to NBP. (Quantitative)(Doc Required)	1
License and Maintenance Support	
Bidder must provide an undertaking that it will not bind NBP for any component upgrades (i.e. OS, Software, Database, Reporting tools etc.) during the period of maintenance & support. However, consent on compatibility will be sought from bidder. Latest version of the solution should be implemented and all patched should be included during contract period under SLA. The methodology for implementing new releases / updates of your software should be described along with specifying user notification process, frequency of updates, update media options and the process by which changes are identified to be included in a new release. (Quantitative)(Doc Required)	1
Bidder must provide the cost of implementation, maintenance and support & warranty (including license, if applicable) for (01) one year after system implementation and user acceptance testing. This is separate from the SLA Agreement, which shall come into effect after completion of the support service period. (Quantitative)(Doc Required)	1
"Bidder must provide cost of a support and maintenance (including license, if applicable) of proposed solution for two (02) consecutive years after the date of expiry of 1st year contract period. It is on bank’s discretion to opt for 2nd and 3rd year support and maintenance agreement." (Quantitative)(Doc Required)	1
Training	
Bidder must provide comprehensive training (functional + technical) to business as well as IT users of NBP on the proposed solution. Details of high level Training Plan / Schedule should be provided by the Bidder with the proposal. (Quantitative)(Doc Required)	1

Bidder must provide undertaking that whenever, there will be new release the bidder will also provide modified desktop manuals, training manuals and user manuals as part of maintenance agreement signed between NBP & Bidder. (Quantitative)(Doc Required)	1
Bidder must provide training sessions for NBP staff as trainers and course creators including video-recording and editing of lectures with hands on experience. (Quantitative)(Doc Required)	1
Bidder must provide Training Guides, Trainer’s guides and Frequently Asked Questions for learners (in both Urdu and English Languages) for the proposed / implemented solution. (Quantitative)(Doc Required)	1
Bidder must provide architecture diagram with process flow of application internal and external integration technically and logically with detailed briefing. (Quantitative)(Doc Required)	1
Security	
System must have ability to define new roles and privileges and assign multiple roles and privileges to the users. Services Menu of users on interface should be based on assigned privileges only. (Quantitative)(Doc Required)	1
System must support single sign-on to access all granted modules of proposed System i.e. Separate login should not be required to access modules of proposed System individually. (Quantitative)(Doc Required)	1
Have capability to disallow multiple concurrent sessions of User-id. (Quantitative)(Doc Required)	1
Support automatic log-off or time-out the session after a defined configurable period of time. (Quantitative)(Doc Required)	1
Be able to block / unblock any user through centralized user management interface. (Quantitative)(Doc Required)	1
Have configuration control for allowed login attempts in a day. Number of failed attempts must be controlled through a parameter. (Quantitative)(Doc Required)	1

Have user Password configuration / control parameters which at a minimum include minimum password length -, alphanumeric, auto-reset password (forget password option) / password generation / construction requirements, password change, password expiry period, password change attempts allowed per day, password change on first login, and non-display of password in clear text on any interface / screen. (Quantitative)(Doc Required)	1
"a) All passwords must be stored and transferred in encrypted form and never in clear text. b) Application must have inputter / authorizer function for all administrative and end-user processes ." (Quantitative)(Doc Required)	1
VAPT of application (white box, Black and Grey box penetration testing) by third party is mandatory. Bidder should provide undertaking that it will provide its full support in remediating and fixing all issues that will be reported by ISD and third party company during the Penetration Testing / Ethical Hacking / Web Vulnerability assessment of the proposed System. This exercise will be performed before Go-Live phase. (Quantitative)(Doc Required)	1
System must provide complete audit trail of unauthorized access, rejected sign on attempts, authorization level changes, Alert's definition and issuance, etc. Logs should be maintained for user activity, admin activity, user management activity, security, user login attempts etc. as required by Audit (Quantitative)(Doc Required)	1
"a) System must provide last access time and date upon login, deployment of content and editing, etc. b) System must maintain history of all modifications of roles with date and time stamp and user performing the activity." (Quantitative) (Doc Required)	1
The application server(s) must have support to be exposed on public servers only via authenticated latest versions of SSL/TLS based connections or recommended by banks ISD. (Quantitative)(Doc Required)	1
The bidder must ensure that system should be protected against all kind of vulnerabilities including all kind of virus/hacking/phishing attacks (including but not limited to DDoS, MITM, SQLi, XSS, Malware Attacks etc.) (Quantitative) (Doc Required)	1
There must be no provision for creation of anonymous accounts within application. (Quantitative)(Doc Required)	1

Maker-checker functionality must be available for User Access Management and activities related to Security Parameterization. (Quantitative)(Doc Required)	1
Application source code must not be accessible to Administrators. (Quantitative)(Doc Required)	1
Administrative accounts must not have access to logs of their own activities. (Quantitative)(Doc Required)	1
All default access capabilities (including passwords) must be changeable. (Quantitative)(Doc Required)	1
Application must be able to auto disable users not logged in to the system for certain period of days (configurable). (Quantitative)(Doc Required)	1
Application system must generate reports for User List, Invalid Login Details with defined Time Duration, Changes in User Rights, 60/90 Day Login Details. (Quantitative)(Doc Required)	1
HTTPS protocol must be implemented. (Quantitative)(Doc Required)	1
Application time must be synchronized with NTP Server. (Quantitative)(Doc Required)	1
Errors should reveal only necessary information without disclosing any internal system detail. (Quantitative)(Doc Required)	1
"a) Passwords or keys must not be hardcoded within application. b) User credentials must not be cached within application. c) Application must not allow creating more than one User ID with same name." (Quantitative)(Doc Required)	1
Any modification of user password must be notified to user via registered Email ID. (Quantitative)(Doc Required)	1
Adequate input filtering controls must be in place to address SQL injection, XSS, RCE and unauthorized file inclusion threats. (Quantitative)(Doc Required)	1
Validations performed at client end must also be performed at server end. (Quantitative)(Doc Required)	1

The bidder must apply security patches in line with service level agreement as soon as patches are available for new vulnerabilities disclosed via CVE no. etc. in technologies/systems which are the part of proposed solution’s architecture. (Quantitative)(Doc Required)	1
"a) User’s credentials and private information such as PII & profile details must not be accessible via browser’s local storage / session storage after the user logs out from application. b) The logging system in proposed solution must have the capability to integrate with standard security monitoring tools/solutions such as SIEM (IBM QRadar, Guardium, Splunk, AlienVault etc.)" (Quantitative)(Doc Required)	1
The database platform must support password configuration / control parameters for database users, which at a minimum includes: minimum password length (i.e. 8 characters length for standard users and 12 characters for administrative/privilege users), alphanumeric with special characters, failed login attempts, password life and password history. (Quantitative)(Doc Required)	1
The database must have capability to enable/generate a comprehensive audit trail, which includes all types of database user’s activities/events and provide integration with third party database security and SIEM solutions. (Quantitative)(Doc Required)	1
"a) The database platform must have capability to change passwords of default and unused database accounts. b) The database should provide best-practice security configuration as per industry leading compliance standards, such as CIS benchmarks etc." (Quantitative)(Doc Required)	1
The database platform must provide native capability of data encryption for sensitive data. Database encryption should be flexible to implement on complete database, table space or at column level. In addition, Database should be flexible to support integration with any 3rd party database encryption solutions. (Quantitative)(Doc Required)	1
The database must provide native capability of data redaction/masking for sensitive data. In addition, Database should be flexible to support integration with any 3rd party data masking/redaction solutions. (Quantitative)(Doc Required)	1
The database must provide role-based-access control at the granular level and allow database administrator to centrally manage roles and privileges of database users. (Quantitative)(Doc Required)	1

Solution Stability and Business Continuity & Contingency Plan- Disaster Recovery Plan	
"a) Escalation process against incident Management , for immediate repair actions in the event of application failure causing an interruption in service. Incident management plan to be provided as well b) Availability of releases / patches which are critical for system stability / security. c) Bidder must provide full support and manuals to setup Application’s disaster recovery site and both Application and Database replication." (Quantitative)(Doc Required)	1
"a) Bidder must to assist NBP in connecting the proposed system with the NBP'S Disaster recovery site. b) Proposed system must include details / SOPs of back up System and mechanism to switch to disaster recovery site." (Quantitative) (Doc Required)	1
"a) System Backup Mechanism must be provided with step-wise procedure document for execution of the same. b) Proposed system must include details of set up required for high availability with Active-Active solution." (Quantitative) (Doc Required)	1
"a) The System Architecture must be based on the principles of performance, scalability and security. b) The System deployment must consider high - availability and DR environment with 99.99% uptime." (Quantitative)(Doc Required)	1
"a) If application is version based then proper version management must be available and documented. b) The System must be able to support any remote connectivity software chosen by NBP in case remote access is required for any operation." (Quantitative)(Doc Required)	1
Other Technical Requirement	
The Proposed Solution must be compatible with, but not limited to, these browsers: Microsoft edge, Google Chrome, and Mozilla Firefox. (Quantitative)(Doc Required)	1
"a) Bidder must provide one solution for Trade Ops, Compliance & Risk Management. b) The Proposed Solution must support latest version of database platforms like Oracle and MS SQL Server. NBP will decide which database to select and proceed." (Quantitative)(Doc Required)	1

"The Proposed Solution must 1. Be able to be deployed as Container based and 2. Be able to be hosted on MS Windows and Linux VM and 3. Be able to be hosted on Intel based hardware with latest MS Windows and Linux operating systems. Deployment model will be at NBP’s discretion." (Quantitative)(Doc Required)	1

Required Services

Positions Without Lots :

Position	Delivery Schedule	Quantity	Bid Security
Trade Based Money Laundering (TBML)	**Address:** The Wing Head CFT & Saction, Compliance Group, 10th Floor, National Bank of Pakistan, Head Office Building, Karachi. **Schedule:** 15 Days **Quantity:** 01/job	1/job	1000000 PKR

Related Services :

No

Services Specifications

Positions Without Lots :

Position: Trade Based Money Laundering (TBML)

Specifications / Requirements:

"As per the current practice which is in line with Regulatory guidelines given in Framework for Managing Trade Based Money Laundering and Terrorist Financing-2019, the bank is using different manual controls and processes in some areas to monitor the TBML risk. However, to further strengthen the controls and processes to counter Trade Based Money Laundering (TBML) in line with EPD Circular Letter No. 08 dated August 12, 2025, we need to acquire a robust and comprehensive system for Monitoring of Trade Based Money Laundering. This system will enable us to streamline our compliance efforts, capture relevant data, consolidate information, and facilitate informed decision-making in different areas of TBML. The areas of TBML which requires to be further strengthen by implementing system controls are Price Due Diligence, Vessel Tracking, Container Tracking, Dual Use Goods, TBML Scenarios, Trade Documents Validation, MIS & Dashboards, Integration with Bank Systems etc."

Scope of Work

As per the current practice which is in line with Regulatory guidelines given in Framework for Managing Trade Based Money Laundering and Terrorist Financing-2019, the bank is using different manual controls and processes in some areas to monitor the TBML risk.

However, to further strengthen the controls and processes to counter Trade Based Money Laundering (TBML) in line with EPD Circular Letter No. 08 dated August 12, 2025, we need to acquire a robust and comprehensive system for Monitoring of Trade Based Money Laundering. This system will enable us to streamline our compliance efforts, capture relevant data, consolidate information, and facilitate informed decision-making in different areas of TBML.

The areas of TBML which requires to be further strengthen by implementing system controls are Price Due Diligence, Vessel Tracking, Container Tracking, Dual Use Goods, TBML Scenarios, Trade Documents Validation, MIS & Dashboards, Integration with Bank Systems etc.

Price Schedule

For Individual Positions

#	Position Title	Quantity	Unit Price (PKR)	Total Price (PKR)	Delivery Location	Delivery Period / Year	Country of Origin
1							
2							

For Lots

#	Lot Title	Total Lot Price (PKR)	Country of Origin
1	[Lot 1 Title]		

PUBLIC PROCUREMENT REGULATORY AUTHORITY
(PPRA)
EPADS

General Conditions of Contract

A. General

1. **Definitions**

1.1. Unless the context otherwise requires, the following terms whenever used in this Contract shall have the same meaning and shall be interpreted as indicated

1.1.1. “Applicable Law” means the laws and any other instruments having the force of law in the Government’s Country, or in such other country as may be specified in the Special Conditions of the Contract (SC), as they may be issued and in force from time to time;

1.1.2. “The Contract” means an agreement enforceable by law;

1.1.3. “The Contract Price” means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations;

1.1.4. “The Services” means the work to be performed by the Contractor pursuant to this Contract and as prescribed in the Specifications and Schedule of Activities included in the Contractor’s Bid;

1.1.5. “Ancillary Services” means those services ancillary to the provision of Services, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Contractor covered under the Contract;

1.1.6. “GCC” means the General Conditions of Contract contained in this section;

1.1.7. “SCC” means the Special Conditions of Contract by which the GCC may be amended or supplemented;

1.1.8. **“**Day” means calendar day unless indicated otherwise;

1.1.9. “Effective Date” means the date on which this Contract comes into force and effect;

1.1.10. “The Contractor” means the individual or corporate body whose Bids to provide the Services has been accepted by the Procuring Agency;

1.1.11. “The Project Site,” where applicable, means the place or places named in Bid Data Sheet and technical Specifications;

1.1.12. “Government” means the Government of Pakistan;

1.1.13. “Local Currency” means the currency of Pakistan;

1.1.14. “In Writing” means communicated in written form with proof of receipt;

1.1.15. “Completion Date” means the date of completion of the Services by the Contractor as certified by the Procuring Agency;

1.1.16. “Foreign Currency” means any currency other than the currency of the country of the Procuring Agency;

1.1.17. “Party” means the Procuring Agency or the Contractor, as the case may be, and “Parties” means both of them;

1.1.18. "Service" means any object of procurement other than goods or works;

1.1.19. “Subcontractor” means any entity to which the Bidder subcontracts any part of the Services.

2. **Applicable Law**

2.1. The contract shall be governed and interpreted in accordance with the laws of Pakistan, unless otherwise specified in SCC.

3. **Language**

3.1. The Contract as well as all correspondence and documents relating to the Contract exchanged between the Contractorand the Procuring Agency, shall be written in the **English language** unless otherwise stated in the **SCC** . Supporting documents and printed literature that are part of the Contract may be in another language provided these are accompanied by an accurate translation of the relevant passages in English, in which case, for purposes of interpretation of the Contract, this translation shall govern.

4. **Notices**

4.1. Any notice, request, or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the **SCC**.

5. **Location**

5.1. The Services shall be performed at such locations as the Procuring Agency may approve and as specified in **SCC.**

6. **Authorized Representatives / Authority of Member in charge**

6.1. Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Procuring Agency or the Contractor may be taken or executed by the officials specified in the **SCC**.

B. Commencement, Completion, Modification, and Termination of Contract

7. **Effectiveness of Contract**

7.1. This Contract shall come into effect on the date the Contract is signed by both parties and such other later date as may be stated in the **SCC.**

8. **Commencement of Services**

8.1. The Contractor shall confirm availability of Key Experts and begin carrying out the Services not later than the number of days after the Effective Date specified in the **SCC.**

9. **Program schedule**

9.1. Before commencement of the Services, the Contractor shall submit to the Procuring Agency for approval a Program showing the general methods, arrangements, order and timing for all activities. The Services shall be carried out in accordance with the approved Program as updated.

10. **Starting Date/Expiration Date**

10.1. The Contractor shall start carrying out the Services Five (05) days after the date the Contract becomes effective, or at such other date as may be specified in the **SCC.**

10.2. Unless terminated earlier pursuant to Clause **GCC 14** hereof, this Contract shall expire at the end of such time period after the Effective Date as specified in the **SCC.**

11. **Entire Agreement**

11.1. This Contract contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

12. **Modification**

12.1. Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any modification(s) or variation(s) made by the other Party.

12.2. In cases of any modification(s) or variation(s), the prior written consent of the Procuring Agency is required.

13. **Force Majeure**

13.1. **Definition**

For the purposes of this Contract, “Force Majeure” means an event which is beyond the reasonable control of a Contractor and which makes a Contractor’s performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

13.2. **No Breach of Contract**

The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

13.3. **Extension of Time**

Any period within which a Contractor shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

13.4. **Payments**

During the period of their inability to perform the Services as a result of an event of Force Majeure, the Contractor shall be entitled to continue to be paid under the terms of this Contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the Services and in reactivating the Service after the end of such period.

14. **Termination**

14.1. **By the Procuring Agency**

The Procuring Agency may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause. In such an occurrence the Procuring Agency shall give at least thirty (30) calendar days' written notice of termination to the Contractor in case of the events referred to in (a) through (d); at least sixty (60) calendar days' written notice in case of the event referred to in (e);

14.1.1. If the Contractor fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice of suspension;

14.1.2. If the Contractor becomes (or, if the Contractor consists of more than one entity, if any of its members becomes) insolvent or bankrupt or enter into any agreements with their creditors for relief of debt or take advantage of any law for the benefit of debtors or go into liquidation or receivership whether compulsory or voluntary;

14.1.3. If the Contractor fails to comply with any final decision reached as a result of arbitration proceedings;

14.1.4. If, as the result of Force Majeure, the Contractor is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;

14.1.5. If the Procuring Agency, in its sole discretion and for any reason whatsoever, decides to terminate this Contract;

14.2. **By the Contractor**

The Contractor may terminate this Contract, by not less than thirty (30) calendar days' written notice to the Procuring Agency, in case of the occurrence of any of the events specified in paragraphs (a) through (d) of this Clause.

14.2.1. If the Procuring Agency fails to pay any money due to the Contractor pursuant to this Contract and not subject to dispute within forty-five (45) calendar days after receiving written notice from the Contractor that such payment is overdue;

14.2.2. If, as the result of Force Majeure, the Contractor is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;

14.2.3. If the Procuring Agency fails to comply with any final decision reached as a result of arbitration;

14.2.4. If the Procuring Agency is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Bidder may have subsequently approved in writing) following the receipt by the Procuring Agency of the Contractor's notice specifying such breach.

C. Obligations of the Contractor

15. **General**

15.1. **Standard of Performance**

15.1.1. The Contractor shall perform the Services and carry out the Services with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Contractor shall always act, in respect of any matter relating to this Contract or to the Services, as a faithful adviser to the Procuring Agency, and shall at all times support and safeguard the Procuring Agency's legitimate interests in any dealings with the third parties;

15.1.2. The Contractor shall employ and provide such qualified and experienced Experts and Sub-Contractors as are required to carry out the Services.

15.2. **Law Applicable to Services**

The Contractor shall perform the Services in accordance with the Contract and in accordance with the Law of Pakistan and shall take all practicable steps to ensure that any of its Experts and Sub-Bidders, comply with the Applicable Law.

16. **Conflict of Interests**

16.1. **Contractor Not to Benefit from Commissions and Discounts**

The remuneration of the Contractor shall constitute the Contractor's sole remuneration in connection with this Contract or the Services, and the Contractor shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Contractor shall use their best efforts to ensure that the Personnel, any Subcontractors, and agents of either of them similarly shall not receive any such additional remuneration.

16.2. **Contractor and Affiliates Not to be Otherwise Interested in Project**

The Contractor agree that, during the term of this Contract and after its termination, the Contractor and its affiliates, as well as any Subcontractor and any of its affiliates, shall be disqualified from providing Services (other than the Services and any continuation thereof) for any project resulting from or closely related to the Services.

16.3. **Prohibition of Conflicting Activities**

Neither the Bidder nor its Subcontractors nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

16.3.1. during the term of this Contract, any business or professional activities in the Government's country which would conflict with the activities assigned to them under this Contract;

16.3.2. during the term of this Contract, neither the Contractor nor their Subcontractors shall hire public employees in active duty or on any type of leave, to perform any activity under this Contract;

16.3.3. after the termination of this Contract, such other activities as may be specified in the **SCC.**

17. **Insurance to be Taken Out by the Contractor**

17.1. The Contractor(a) shall take out and maintain, and shall cause any Subcontractors to take out and maintain, at its (or the Sub-contractors', as the case may be) own cost but on terms and conditions approved by the Procuring Agency, insurance against the risks, and for the coverage, as shall be specified in the **SCC**; and (b) at the Procuring Agency's request, shall provide evidence to the Procuring Agency showing that such insurance has been taken out and maintained and that the current premiums have been paid.

18. **Contractor's Actions Requiring Procuring Agency's Prior Approval**

18.1. The Contractor shall obtain the Procuring Agency's prior approval in writing before taking any of the following actions:

18.1.1. appointing such members of the Personnel not provided by the Contractor;

18.1.2. changing the Program of activities; and

18.1.3. any other action that may be specified in the **SCC.**

19. **Reporting Obligations**

19.1. The Contractor shall submit to the Procuring Agency the reports and documents in the numbers, and within the periods as prescribed by the Procuring Agency.

20. **Liquidated Damages**

20.1. **Payments of Liquidated Damages**
The Contractor shall pay liquidated damages to the Procuring Agency at the rate per day stated in the **SCC** for each day that the Completion Date is later than the Intended Completion Date. The total amount of liquidated damages shall not exceed the amount defined in the **SCC**. The Procuring Agency may deduct liquidated damages from payments due to the Contractor. Payment of liquidated damages shall not affect the Contractor's liabilities.

20.2. **Correction for Over-payment**
If the Intended Completion Date is extended after liquidated damages have been paid, the Procuring Agency shall correct any overpayment of liquidated damages by the Contractor by adjusting the next payment certificate. The Contractor shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment, at the rates specified in **SCC.**

20.3. **Lack of performance penalty**

If the Contractor has not corrected a Defect within the time specified in the Procuring Agency's notice, a penalty for Lack of performance will be paid by the Contractor. The amount to be paid will be calculated as a percentage of the cost of having the Defect corrected, assessed as specified in the Contractor

21. **Performance Guarantee**

21.1. Within the time stipulated in the acceptance letter from the Procuring Agency, the successful Bidder shall furnish the Performance Guarantee in shape and amount **specified in SCC.**

21.2. The proceeds of the Performance Guarantee shall be payable to the Procuring agency as compensation for any loss resulting from the Supplier's failure to complete its obligations under the Contract.

21.3. The Performance Guarantee shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Procuring agency and shall be in the acceptable form as specified in **SCC**.

21.4. The Performance Guarantee will be discharged by the Procuring agency and returned to the Supplier not later than thirty (30) days following the date of completion of the Supplier's performance obligations under the Contract, including any warranty obligations, unless otherwise **specified in SCC.**

22. **Sustainable Procurement**

22.1. The Contractor shall conform to the sustainable procurement contractual provisions, if and as specified in the **SCC.**

D. Contractor's Personnel

23. **Description of Personnel**

23.1. The titles, agreed job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the Services of the Contractor's Key Personnel. The Key Personnel listed by title as well as by name are hereby approved by the Procuring Agency.

24. **Removal and / or Replacement of Personnel**

24.1. Except as the Procuring Agency may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Contractor, it becomes necessary to replace any of the Key Personnel, the Contractor shall provide as a replacement a person of equivalent or better qualifications.

24.2. If the Procuring Agency finds that any of the Personnel have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Contractor shall, at the Procuring Agency's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the Procuring Agency.

24.3. The Contractor shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.

E. Obligations of the Procuring Agency

25. **Change in the Applicable Law**

25.1. If, after the date of this Contract, there is any change in the Applicable Law with respect to taxes and duties which increases or decreases the cost of the Services rendered by the Contractor, then the remuneration and reimbursable expenses otherwise payable to the Contractor under this Contract shall be increased or decreased accordingly by agreement between the Parties, and corresponding adjustments shall be made to the amounts referred in the **SCC.**

26. **Services and Facilities**

26.1. The Procuring Agency shall make available to the Contractor and the Experts, for the purposes of the Services and free of any charge, the services, facilities and property described in the Terms of Reference, at the times and in the manner specified in the Terms of Reference.

26.2. In case that such services, facilities and property shall not be made available to the Contractor, the Parties shall agree on (i) any time extension that it may be appropriate to grant to the Contractor for the performance of the Services, (ii) the manner in which the Contractor shall procure any such services, facilities and property from other sources, and (iii) the additional payments, if any, to be made to the Contractor as a result thereof.

F. Payments to the Contractor

27. **Contract Price**

27.1. The price payable shall be in Pakistani Rupees unless otherwise specified in the **SCC**.

28. **Terms and Conditions of Payment**

28.1. Payments will be made to the Contractor according to the payment schedule stated in the **SCC** and as per actual invoice submitted by the Contractor.

28.2. Unless otherwise stated in the **SCC**, the advance payment shall be made against the provision by the Contractor of a bank guarantee for the same amount, and shall be valid for the period stated in the **SCC.** Any other payment shall be made after the conditions listed in the **SCC** for such payment have been met, and the Contractor have submitted an invoice to the Procuring Agency specifying the amount due.

29. **Quality Control Identifying Defects**

29.1. The principle and modalities of Inspection of the Services by the Procuring Agency shall be as indicated in the **SCC.** The Procuring Agency shall check the Contractor's performance and notify him of any Defects that are found. Such checking shall not affect the Contractor's responsibilities. The Procuring Agency may instruct the Contractor to search for a Defect and to uncover and test any service that the Procuring Agency considers may have a Defect. Defect Liability Period is as defined in the **SCC**.

30. **Correction of Defects, and Lack of Performance Penalty**

30.1. The Procuring Agency shall give notice to the contractor of any Defects before the end of the Contract. The Defects liability period shall be extended for as long as Defects remain to be corrected.

30.2. Every time notice a Defect is given; the contractor shall correct the notified Defect within the length of time specified by the Procuring Agency's notice.

30.3. If the contractor has not corrected a Defect within the time specified in the Procuring Agency's notice, the Procuring Agency will assess the cost of having the Defect corrected, the contractor will pay this amount, and a Penalty for Lack of Performance.

31. **Settlement of Disputes Amicable Settlement**

31.1. The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.

32. **Dispute Settlement**

32.1. **Arbitration**

If any dispute of any kind whatsoever shall arise between the procuring agency and the contractor in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity or termination, or the execution of the contract, the parties shall seek to resolve any such dispute or difference by mutual consultation. If the parties fail to resolve such a dispute or difference even after negotiations or mediation, then the dispute shall be referred within fourteen (14) days in writing by either party to the Arbitrator, with a copy to the other party.

Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with **GCC sub-clause 32.1**, shall be finally settled by arbitration. Arbitration may be commenced prior to or after completion of the Contract. Arbitration proceedings shall be conducted in accordance with Arbitration Act 1940.

Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless otherwise agreed. The Procuring Agency shall continue to pay the Contractor any undisputed amounts due under the Contract during the resolution of any dispute.

Special Conditions of Contract

SECTION VIII. SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the Conditions of Contract. The corresponding clause number of the GCC is indicated in parentheses.

Number of GC Clause

Amendments of, and Supplements to, Clauses in the General Conditions of Contract

Definitions

The Procuring Agency is: National Bank of Pakistan (Compliance Group), SVP The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.

The Supplier is:

The title of the subject procurement is:Trade Based Money Laundering (TBML)

Number of GC Clause 2

Applicable/Governing Law:

The Contract shall be interpreted in accordance with the laws of Islamic Republic of Pakistan

Number of GC Clause 3

Language:

The language of the Contract, all correspondence and communications to be given, and all other documentation to be prepared and supplied under the Contract shall be in **English.**

Number of GC Clause 4

Notices:

The addresses for the notices are:

Procuring Agency:

National Bank of Pakistan (Compliance Group), SVP
The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.
+92-213-890-2267
teemar@nbp.com.pk

Contractor/ Bidder:

[Name, address and telephone number].

The Contractor/ Bidder’s Representative(s)

[Name, address, telephone number and e-mail address]

Number of GC Clause 6.1

The Authorized Representatives are:

For the Procuring Agency:

National Bank of Pakistan (Compliance Group), SVP
The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.
+92-213-890-2267
teemar@nbp.com.pk

For the Bidder:

Name: ……

Designation: ……..

Address: ……..

Number of GC Clause 7

Effectiveness of the contract

The Contractor/Bidder shall be effective within ….. days from the date of signature of the Contract by both parties

Number of GC Clause 8

Commencement of Contract:

The Contractor/ Bidder shall provide Non-Consultancy Services from the effective date of contract.

Number of GC Clause 10.2

Expiration of Contract:

The time period shall be …….

Number of GC Clause 14

Termination

In the event of termination of the contract due to any reason as already defined in the General Conditions of Contract, the Bidder shall be responsible for providing to the Authority the Services till the time of alternate arrangements.

Number of GC Clause 16

Conflict of Interest:

The Procuring Agency reserves the right to determine on a case-by-case basis whether the Bidder should be disqualified from providing services due to a conflict of a nature described in Clause GCC C2**.**

Number of GC Clause 20

Liquidated Damages

If the Bidder fails to provide services as required under the contract or in case of any data loss/data breach or any incident compromising the data security or other such failures related to any services, the Bidder shall pay to the Procuring Agency as Liquidated Damages at a rate of **0.00%** to **0.00%** of the Contract value, in accordance with the extent of performance failure & the cost of investigating such incidents as judged by the Authority.

Number of GC Clause 21

Performance Guarantee:

The amount of performance guarantee shall be 10.00% of the contract price in acceptable form of Banker's Cheque, Bank Guarantee

Number of GC Clause 27

Currency of Payment:

All the payment to be released to the contractor/Bidder shall be in Pakistani Rupees.

Number of GC Clause F

Payment terms:

Payment will be made to the Bidder against the procured Goods and services according to the actual invoice or running bills submitted by the Bidder against the services provided within the time given in the conditions of the contract.

Number of GC Clause F

Identifying Defects:

The Authority reserves the right at any time to inspect the premises of the provider to inspect the goods and monitor the goods being provided.

Delivery & Documents

Confirmation of Licenses of Complete Proposed Solution as mentioned in Technical Requirements.

Product Complete Technical & User level documentation (For example; Software Requirement Specifications, Design Document, Database ERD, Installation Guide, User Manual, Train the Trainer Manual etc.)

Invoice Showing detailed breakup.

Number of GC Clause F 5 & 6

Following is the guidance for Dispute Resolution

i. If any dispute of any kind whatsoever shall arise between the Authority and the Bidder in connection with or arising out of the Contract, including without prejudice to the generality of foregoing, any question regarding its existence, validity, termination and the execution of the Contract – whether during developing phase or after their completion and whether before or after the termination, abandonment or breach of the Contract – the parties shall seek to resolve any such dispute or difference by mutual diligent negotiations in good faith within 14 (fourteen) days following a notice sent by one Party to the other Party in this regard**.**

ii. At future of negotiation the dispute shall be resolved through mediation and mediator shall be appointed with the mutual consent of the both parties**.**

iii. At the event of failure of mediation to resolve the dispute relating to this contract such dispute shall finally be resolved through binding Arbitration by sole arbitrator in accordance with Arbitration Act 1940. The arbitrator shall be appointed by mutual consent of the both parties**.** The Arbitration shall take place in Islamabad, Pakistan and proceedings will be conducted in English language.

iv. The cost of the mediation and arbitration shall be shared by the parties in equal proportion however the both parties shall bear their own costs and lawyer's fees regarding their own participation in the mediation and arbitration. However, the Arbitrator may make an award of costs upon the conclusion of the arbitration making any party to the dispute liable to pay the costs of another party to the dispute**.**

v. Arbitration proceedings as mentioned in the above clause regarding resolution of disputes may be commenced prior to, during or after completion of the contract.

Notwithstanding any reference to the arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree that the Authority shall pay the Bidder any monies due to the Bidder.

Arbitrator's fee:

The fee shall be specified in Pak Rupees, as determined by the Arbitrator, which shall be shared equally by both parties**.**

Appointing Authority for Arbitrator:

By the Mutual Consent or in accordance with the provisions of Arbitration Act, 1940, in case the parties fail to reach a consensus on the name of sole arbitrator, any party may submit an application to the Chief Justice Islamabad High Court for appointment of sole arbitrator. The Chief Justice IHC may appoint a former judge of any High Court or Supreme Court as the sole arbitrator to resolve the dispute between the parties.

Rules of procedure for arbitration proceedings:

Any dispute between the Authority and a Bidder who is a national of the Islamic Republic of Pakistan arising in connection with the present Contract shall be referred to adjudication or arbitration in accordance with the laws of the Islamic Republic of Pakistan including Arbitration Act 1940, however above provision shall prevail in referring the case to the Arbitrator.

Place of Arbitration and Award:

The arbitration shall be conducted in English language and place of arbitration shall be at Islamabad. The award of the arbitrator shall be final and shall be binding on the parties.

Bid Securing Declaration

Form 9: Bid Securing Declaration

Date: *[insert date (as day, month and year)]*

Bid No.:***P97471***

To: **National Bank of Pakistan (Compliance Group), SVP The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.**

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid Securing Declaration.

We accept that we will be blacklisted and henceforth cross debarred for participating in respective category of public procurement proceedings for a period of (not more than) six months, if fail to abide with a bid securing declaration, however without indulging in corrupt and fraudulent practices, if we are in breach of our obligation(s) under the Bid conditions, because we:

1. have withdrawn or modified our Bid during the period of Bid Validity specified in the Form of Bid;

2. Disagreement to arithmetical correction made to the Bid price; or

3. having been notified of the acceptance of our Bid by the Procuring Agency during the period of Bid Validity, (i) failure to sign the contract if required by Procuring Agency to do so or (ii) fail or refuse to furnish the Performance Security or to comply with any other condition precedent to signing the contract specified in the Bidding Documents.

We understand this Bid Securing Declaration shall expire if we are not the successful

Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight (28) days after the expiration of our Bid.

Contract Form

SECTION IX: CONTRACT FORMS

THIS AGREEMENT made the _____ day of _____ 20_____ between **National Bank of Pakistan (Compliance Group), SVP The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.**

(hereinafter called "the Procuring Agency") of the one part and *[name of Bidder]* of *[city and country of Bidder]* (hereinafter called "the Bidder") of the other part:

WHEREAS the Procuring Agency invited Bids for provision of goods, viz., **Trade Based Money Laundering (TBML) (*P97471*)** and has accepted a Bids by the Bidder for the provision of Goods in the sum of *[contract price in words and figures]* (hereinafter called "the Contract Price").

NOW THIS CONTRACT WITNESSETH AS FOLLOWS:

1. In this Contract words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Contract, In the event of any ambiguity or conflict between the Contract Documents listed below, the order of precedence shall be the order in which the Contract Documents are listed below:-

1. This form of Contract;
2. the Form of Bids and the Price Schedule submitted by the Bidder;
3. the Schedule of Requirements;
4. the Technical Specifications;
5. the Special Conditions of Contract;
6. the General Conditions of the Contract;
7. the Procuring Agency's Letter of Acceptance; and
8. [*add here: any other documents*]

3. In consideration of the payments to be made by the Procuring Agency to the Bidder as hereinafter mentioned, the Bidder hereby covenants with the Procuring Agency to provide the Goods related services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Procuring Agency hereby covenants to pay the Bidder in consideration of the provision of Goods and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Contract to be executed in accordance with their respective laws the day and year first above written.

Signed, sealed, delivered by _____the _____ (for the Procuring Agency)

Witness to the signatures of the Procuring Agency:

……

Signed, sealed, delivered by _____the _____ (for the Procuring Agency)

Witness to the signatures of the Bidder: ……

Integrity Pact

Integrity Pact

DECLARATION OF FEES, COMMISSION AND BROKERAGE ETC. PAYABLE BYTHE SUPPLIERS OF GOODS, SERVICES & WORKS IN CONTRACTS WORTH RS.10.00 MILLION OR MORE

Contract Number: Contract Value: Contract Title:

Dated:

[Name of Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing [Name of Supplier] represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[Name of Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

[Name of Supplier] accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [Name of Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by [Name of Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

Performance Guarantee Form

Performance Guarantee Form

To: **National Bank of Pakistan (Compliance Group), SVP The Office of Departmental Head Tender, Procurement Division-LCMG, 3rd Floor, National Bank of Pakistan, Head Office Building, Karachi.**

WHEREAS *[name of Bidder]* (hereinafter called "the Bidder") has undertaken, in pursuance of Contract No. *[reference number of the contract]* dated *[insert date]* for provision of Goods*(*hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Bidder shall furnish you with a Bank Guarantee by a reputable bank for the sum specified therein as security for compliance with the Bidder's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Bidders guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Bidder, up to a total of *[amount of the guarantee in words and figures]*, and we undertake to pay you, upon your first written demand declaring the Bidder to be in default under the Contract and without cavil or argument, any sum or sums within the limits of *[amount of guarantee]* as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the: *[insert date]*

Signature and seal of the Guarantors

_____

[name of bank or financial institution]

_____

[address]

_____

[date}

Annexure

SBD

Information (Read-Only)

See Form Under Additional Forms and Documents: **SBD** (page number: 82)

Techincal Submission Req.

Technical Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Techincal Submission Req.** (page number: 275)

Procurement Forms

Past Experience and Completed Contracts

Bidder must provide 03 (three) CV's/Profile of their proposed implementation and configuration team which should be employees of the company since last one year and must have relevant experience for proposed solution.

See Form Under Additional Forms and Documents: **Past Experience and Completed Contracts** (page number: 317)

Historical Contract Non-Performance, and Pending Litigation and Litigation History

Undertaking on Estamp paper amounting to PKR 500/- stating that the bidder is not blacklisted byany Goverment insitution (Federal/ Provincial)

See Form Under Additional Forms and Documents: **Historical Contract Non-Performance, and Pending Litigation and Litigation History** (page number: 318)

Current Contracts and Their Progress

Attach agreement/Work Orderongoing/completed contracts of simlarnature.

See Form Under Additional Forms and Documents: **Current Contracts and Their Progress** (page number: 320)

Financial Capacity and Net Worth Evaluation Form

Bidder must provide audited Profit & Loss (Income Statement) showing Sale volume of company of at least Rs.50 Million in each last 3 years.

See Form Under Additional Forms and Documents: **Financial Capacity and Net Worth Evaluation Form** (page number: 321)

Average Annual Turnover

See Form Under Additional Forms and Documents: **Average Annual Turnover** (page number: 323)

PUBLIC PROCUREMENT REGULATORY AUTHORITY
(PPRA)
EPADS

Additional Forms and Documents

BIDDING DOCUMENT
FOR
TRADE BASED MONEY LAUNDERING SYSTEM
SINGLE STAGE TWO ENVELOPE

Table of Contents

BIDDING PROCEDURE & REQUIREMENTS
SECTION I: INVITATION TO BIDS

INVITATION TO BID THROUGH EPADS

PROCUREMENT OF TRADE BASED MONEY LAUNDERING SYSTEM

1. National Bank of Pakistan, one of the largest commercial banks operating in Pakistan, invites bids through E-Pak Acquisition and Disposal System (EPADS) from suppliers / firms registered with Income Tax and Sales Tax Departments and who are on Active Taxpayers List of the Federal Board of Revenue and having registered office, for PROCUREMENT OF **TRADE BASED MONEY LAUNDERING SYSTEM**

2. Bidding documents, containing detailed terms and conditions, can be downloaded from https://eprocure.gov.pk free of cost. Bids should be submitted electronically **ONLY** through EPADS. Manual submission of bids is **NOT** allowed. For registration and training on EPADS or in case of any technical difficulty in using EPADS, prospective bidders may contact PPRA office ,1st Floor, FBC building sector G-5/2, Islamabad. Or Contact number 051-111-137-237, 051-9205728.

3. The bids, prepared in accordance with the instructions in the bidding documents, must be submitted on EPADS by XXXXX, 2025 3:00PM. Bids will be opened on the same day at 3:30PM.

Note:

1. All interested bidders must register themselves at EPADS at: https://eprocure.gov.pk/#/supplier/registration. No physical bid shall be entertained.
2. Original Bid Security instrument MUST BE submitted to the undersigned office before the online submission deadline of the bid.
3. Pre-bid meeting will be held on _____

(Divisional Head)
Procurement Division,
Logistics, Communications & Marketing Group,
National Bank of Pakistan
3rd Floor, Head Office Building, Karachi.
021-99220331, 021-38902647

SECTION II: INSTRUCTION TO BIDDERS (ITBs)

INTRODUCTION

1. Scope of Bid	1.1	The Procuring Agency (PA), as indicated in the Bid Data Sheet (BDS) invites Bids for the Supply and Installation of the Trade Based Money Laundering (TBML) Systems as specified in the BDS and Section V - Technical Specifications & Schedule of Requirements. The successful Bidders will be expected to supply and install the TBML systems within the specified period and timeline(s)
	1.2	Unless otherwise stated throughout this document definitions and interpretations shall be as prescribed in the General Conditions of the Contract (GCC).
2. Source of Funds	2.1	Source of funds is referred in Clause-2 of Invitation for Bids.
3. Eligible Bidders	3.1	A Bidder may be company or firm or public or semi- public agency of Pakistan or any foreign country, or any combination of them with a formal existing agreement (on Judicial Papers) in the form of a joint venture, consortium, or association. In the case of a joint venture, consortium, or association, all members shall be jointly and severally liable for the execution of the Contract in accordance with the terms and conditions of the Contract. The joint venture, consortium, or association shall nominate a Lead Member as nominated in the BDS, who shall have the authority to conduct all business for and on behalf of any and all the members of the joint venture, consortium, or association during the Bidding process, and in case of award of contract, during the execution of contract. *(The limit on the number of members of JV or Consortium or Association may be prescribed in BDS, in accordance with the guidelines issued by the PPRA)*.
	3.2	The appointment of Lead Member in the joint venture, consortium, or association shall be confirmed by submission of a valid Power of Attorney to the Procuring Agency.
	3.3	Verifiable copy of the agreement that forms a joint venture, consortium or association shall be required to be submitted as part of the Bid.
	3.4	Any bid submitted by the joint venture, consortium or association shall indicate the part of proposed contract to be performed by each party and each party shall be evaluated (or post qualified if required) with respect to its contribution only, and the responsibilities of each party shall not be substantially altered without prior written approval of the Procuring Agency and in line with any instructions issued by the Authority.

	3.5	The invitation for Bids is open to all prospective supplier, manufacturers or authorized agents/dealers subject to any provisions of incorporation or licensing by the respective national incorporating agency or statutory body established for that particular trade or business.
	3.6 .	Foreign Bidders must be locally registered with the appropriate national incorporating body or the statutory body, before participating in the national/international competitive tendering with the exception of such procurements made by the foreign missions of Pakistan. For such purpose the bidder must have to initiate the registration process before the bid submission and the necessary evidence shall be submitted to the procuring agency along with their bid, however, the final award will be subject to the complete registration process.
	3.7	A Bidder shall not have a conflict of interest. All Bidders found to have a conflict of interest shall be disqualified. A Bidders may be considered to have a conflict of interest with one or more parties in this Bidding process, if they: a) are associated or have been associated in the past, directly or indirectly with a firm or any of its affiliates which have been engaged by the Procuring Agency to provide consulting services for the preparation of the design, specifications and other documents to be used for the procurement of the TBML systems to be procured under this Invitation for Bids. b) have controlling shareholders in common; or c) receive or have received any direct or indirect subsidy from any of them; or d) have the same legal representative for purposes of this Bid; or e) have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Bid of another Bidder, or f) influence the decisions of the Procuring Agency regarding this Bidding process; or g) Submit more than one Bid in this Bidding process.

	3.8	A Bidder may be ineligible if – a) he is declared bankrupt or, in the case of company or firm, insolvent; b) payments in favor of the Bidder is suspended in accordance with the judgment of a court of law other than a judgment declaring bankruptcy and resulting (in accordance with the national laws) in the total or partial loss of the right to administer and dispose of its property; c) legal proceedings are instituted against such Bidder involving an order suspending payments and which may result, in accordance with the national laws, in a declaration of bankruptcy or in any other situation entailing the total or partial loss of the right to administer and dispose of the property; d) the Bidder is convicted, by a final judgment, of any offence involving professional conduct; (the Bidder is blacklisted and hence debarred due to involvement in corrupt and fraudulent practices, or performance failure or due to breach of bid securing declaration. e) The firm, supplier and contractor is blacklisted or debarred by a foreign country, international organization, or other foreign institutions for the period defined by them.
	3.9	Bidders shall provide to the Procuring Agency evidence of their eligibility, proof of compliance with the necessary legal requirements to carry out the contract effectively.
	3.10	Bidders shall provide such evidence of their continued eligibility to the satisfaction of the Procuring Agency, as the Procuring Agency shall reasonably request.
	3.11	Bidders shall submit proposals relating to the nature, conditions and modalities of sub-contracting wherever the sub-contracting of any elements of the contract amounting to the more than ten (10) percent of the Bid price is envisaged.

4. Eligible Information/ TBML Systems	4.1	For the purposes of these Bidding Documents, the TBML System means all: a) the required information/ TBML technologies, including all information processing and communications-related hardware, software, supplies, and consumable items that the Supplier is required to supply and install under the Contract, plus all associated documentation, and all other materials and goods to be supplied, installed, integrated, and made operational (collectively called "the Goods" in some clauses of the ITB); and b) the related software development, transportation, insurance, installation, customization, integration, commissioning, training, technical support, maintenance, repair, and other services necessary for proper operation of the TBML System to be provided by the selected Bidder and as specified in the Contract.
	4.2	All Information/ TBML System made up of goods and services to be supplied under the contract shall have their origin in eligible source countries, and all expenditures made under the contract will be limited to the supply and installation TBML systems. For purpose of this Bid, ineligible countries are stated in the section-4 titled as "Eligible Countries".
	4.3	For purposes of this Clause, "origin" means the place where the goods and services making TBML System are produced in or supplied from. An TBML System is deemed to be produced in a certain country when, in the territory of that country, through software development, manufacturing, or substantial or major assembly or integration of components, a commercially recognized product result that is substantially different in basic characteristic or in purpose or utility from its component.
	4.4	The nationality of the supplier that supplies and install the TBML System shall not determine the origin of the goods.
	4.5	To establish the eligibility of the Goods and Services making / TBML System, Bidders shall fill the country-of-origin declarations included in the Form of Bid.
	4.6	If so required in the BDS, the Bidder shall demonstrate that it has been duly authorized for the supply and installation of TBML System in Pakistan (or in respective country in case of procurement by the Pakistani Missions abroad), the TBML System indicated in its Bid.
5. One Bid per Bidder	5.1	A bidder shall submit only one Bid, in the same bidding process, either individually as a Bidder or as a member in a joint venture or any similar arrangement.
	5.2	No bidder can be a sub-contractor while submitting a Bid individually or as a member of a joint venture in the same Bidding process.

	5.3	A person or a firm cannot be a sub-contractor with more than one bidder in the same bidding process.
6. Cost of Bidding	6.1	The Bidder shall bear all costs associated with the preparation and submission of its Bid, and the Procuring Agency shall in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

BIDDING DOCUMENTS

7. Contents of Bidding Documents	7.1	The Contents of the Bidding Documents listed below should be read in conjunction with any addenda issued in accordance with ITB 9.2 include: Section I -Invitation to Bids Section II Instructions to Bidders (ITBs) Section III Bid Data Sheet (BDS) Section IV Eligible Countries Section V Technical Specifications, Schedule of Requirements Section VI Forms – Bid Section VII General Conditions of Contract (GCC) Section VIII Special Conditions of Contract (SCC) Section IX Contract Forms
	7.2	The number of copies to be completed and returned with the Bid is specified in the BDS.
	7.4	The Procuring Agency is not responsible for the completeness of the Bidding Documents and their addenda, if they were not obtained directly from the Procuring Agency or the signed pdf version from downloaded from the website of the Procuring Agency. However, Procuring Agency shall place both the pdf and same editable version to facilitate the bidder for filling the forms.
	7.5	The Bidder is expected to examine all instructions, forms, terms and specifications in the Bidding Documents. Failure to furnish all the information required in the Bidding Documents will be at the Bidder's risk and may result in the rejection of his Bid.
8. Clarification of Bidding Documents, Pre- Bid Meeting and Site Visit	8.1	A prospective Bidder requiring any clarification of the Bidding Documents may notify the Procuring Agency in writing or in electronic form that provides record of the content of communication at the Procuring Agency's address indicated in the BDS.

	8.2	The Procuring Agency will within three (3) working days after receiving the request for clarification, respond in writing or in electronic form to any request for clarification provided that such request is received not later than three (03) days prior to the deadline for the submission of Bids as prescribed in ITB 23.1. However, this clause shall not apply in case of alternate methods of Procurement.
	8.3	Copies of the Procuring Agency's response will be forwarded to all identified Prospective Bidders through an identified source of communication, including a description of the inquiry, but without identifying its source. In case of downloading of the Bidding Documents from the website of PA, the response of all such queries will also be available on the same link available at the website.
	8.4	Should the Procuring Agency deem it necessary to amend the Bidding Documents as a result of a clarification, it shall do so following the procedure under ITB 9.
	8.5	If indicated in the BDS, the Bidder's designated representative is invited at the Bidder's cost to attend a pre-Bid meeting at the place, date and time mentioned in the BDS. During this pre-Bid meeting, prospective Bidders may request clarification of the schedule of requirement, the Evaluation Criteria or any other aspects of the Bidding Documents.
	8.6	Minutes of the pre-Bid meeting, if applicable, including the text of the questions asked by Bidders, including those during the meeting (without identifying the source) and the responses given, together with any responses prepared after the meeting will be transmitted promptly to all prospective Bidders who have obtained the Bidding Documents. Any modification to the Bidding Documents that may become necessary as a result of the pre-Bid meeting shall be made by the Procuring Agency exclusively through the use of an Addendum pursuant to ITB 9. Non-attendance at the pre-Bid meeting will not be a cause for disqualification of a Bidder.
	8.7	The Bidder may wish to visit and examine the site or sites of the Information/ TBML System and obtain for itself, at its own responsibility and risk, all information that may be necessary for preparing the bid and entering into the Contract. The costs of visiting the site or sites shall be at the Bidder's own expense.

	8.8	The Procuring Agency will arrange for the Bidder and any of its personnel or agents to gain access to the relevant site or sites, provided that the Bidder gives the Procuring Agency adequate notice of a proposed visit of at least seven (07) days. Alternatively, the Procuring Agency may organize a site visit or visits concurrently with the pre-bid meeting, as specified in the BDS for ITB Clause 8.5. Failure of a Bidder to make a site visit will not be a cause for its disqualification.
	8.9	No site visits shall be arranged or scheduled after the deadline for the submission of the Bids and prior to the award of Contract.
9. Amendment of Bidding Documents	9.1	Before the deadline for submission of Bids, the Procuring Agency for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder or pre-bid meeting may modify the Bidding Documents by issuing addenda.
	9.2	Any addendum issued including the notice of any extension of the deadline shall be part of the Bidding Documents pursuant to ITB 7.1 and shall be communicated in writing or in any identified electronic form that provide record of the content of communication to all the bidders who have obtained the Bidding Documents from the Procuring Agency. The Procuring Agency shall promptly publish the Addendum at the Procuring Agency's web page identified in the BDS: Provided that the bidder who had either already submitted their bid or handed over the bid to the courier prior to the issuance of any such addendum shall have the right to withdraw his already filed bid and submit the revised bid prior to the original or extended bid submission deadline.
	9.3	To give prospective Bidders reasonable time in which to take an addendum/corrigendum into account in preparing their Bids, the Procuring Agency may, at its discretion, extend the deadline for the submission of Bids: Provided that the Procuring Agency shall extend the deadline for submission of Bid, if such an addendum is issued within last three (03) days of the Bid submission deadline.

PREPARATION OF BIDS

10.Language of Bid	10.1	The Bid prepared by the Bidder, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Procuring Agency shall be written in the English language unless otherwise specified in the BDS. Supporting documents and printed literature furnished by the Bidder may be in another language provided they are accompanied by an accurate translation of the relevant pages in the English language unless specified in the BDS, in which case, for purposes of interpretation of the Bidder, the translation shall govern.
11. Documents Constituting the Bid	11.1	The Bid prepared by the Bidder shall constitute the following components: - a) Form of Bid and Bid Prices completed in accordance with ITB 14 and 15; b) Details of the Sample(s) where applicable and requested in the BDS. c) Documentary evidence established in accordance with ITB 13 that the Bidder is eligible and/or qualified for the subject bidding process. d) Documentary evidence established in accordance with ITB 13.3(a) that the Bidder has been authorized by the manufacturer to deliver the goods and services making TBML System into Pakistan, where required and where the supplier is not the manufacturer of those goods and service making TBML System; e) Documentary evidence established in accordance with ITB 12 that the goods and services making TBML System to be supplied by the Bidder are eligible, and conform to the Bidding Documents; f) Bid security or Bid Securing Declaration furnished in accordance with ITB 18; g) Duly Notarized Power of Attorney authorizing the signatory of the Bidder to submit the bid; and h) Any other document required in the BDS.
12. Documents Establishing Eligibility of the TBML System and Conformity to Bidding Documents	12.1	Pursuant to ITB 11, the Bidder shall furnish, as part of its Bid, all those documents establishing the eligibility in conformity to the terms and conditions specified in the Bidding Documents for all goods and services making TBML system which the Bidder proposes to deliver.

	12.2	The documentary evidence of the eligibility of the Information/ TBML System shall consist of a statement in the Price Schedule of the country of origin of the goods and services making TBML System offered which shall be confirmed by a certificate of origin issued at the time of shipment.
	12.3	The documentary evidence of conformity of the goods and services making TBML Systems to the Bidding Documents may be in the form of literature, drawings, and data, and shall consist of: a) a detailed description of the essential technical specifications and performance characteristics of the Goods; b) an item-by-item commentary on the Procuring Agency's Technical Specifications demonstrating substantial responsiveness of the Goods and Services to those specifications, or a statement of deviations and exceptions to the provisions of the Technical Specifications; c) any other procurement specific documentation requirement as stated in the BDS.
	12.4	For purposes of the commentary to be furnished pursuant to ITB 12.3(c) above, the Bidder shall note that standards for workmanship, material, and equipment, as well as references to brand names or catalogue numbers designated by the Procuring Agency in its Technical Specifications, are intended to be descriptive only and not restrictive. The Bidder may substitute alternative standards, brand names, and/or catalogue numbers in its Bid, provided that it demonstrates to the Procuring Agency's satisfaction that the substitutions ensure substantial equivalence to those designated in the Technical Specifications.
	12.6	The required documents and other accompanying documents must be in English. In case any other language than English is used the pertinent translation into English shall be attached to the original version.

13. Documents Establishing Eligibility and Qualification of the Bidder	13.1	Pursuant to ITB 11, the Bidder shall furnish, as part of its Bid, all those documents establishing the Bidder's eligibility to participate in the bidding process and/or its qualification to perform the contract if its Bid is accepted.
	13.2	The documentary evidence of the Bidder's eligibility to Bid shall establish to the satisfaction of the Procuring Agency that the Bidder, at the time of submission of its bid, is from an eligible country as defined in Section-4 titled as "Eligible Countries".
	13.3	The documentary evidence of the Bidder's qualifications to perform the contract if its Bid is accepted shall establish to the satisfaction of Procuring Agency that: a) in the case of a Bidder offering to supply and install TBML System under the contract which the Bidder did not manufacture or otherwise produce, the Bidder has been duly authorized by the Manufacturer or producer to supply and install the information / TBML system in Pakistan; b) the Bidder has the financial, technical, and supply/production capability necessary to perform the Contract, meets the qualification criteria specified in BDS. c) in the case of a Bidder not doing business within Pakistan, the Bidder is or will be (if awarded the contract) represented by an Agent in Pakistan equipped, and able to carry out the Supplier's maintenance, repair, and spare parts-stocking obligations prescribed in the Conditions of Contract and/or Technical Specifications. that the Bidder meets the qualification criteria listed in the Bid Data Sheet.

	13.4	The documentary evidence of conformity of the TBML System to the Bidding Documents shall be in the form of written descriptions, literature, diagrams, certifications, and client references, including: a) the Bidder's technical bid, i.e., a detailed description of the Bidder's proposed technical solution conforming in all material aspects with the Technical Requirements and other parts of these Bidding Documents, overall as well as in regard to the essential technical and performance characteristics of each component making up the proposed Information/ TBML System; b) an item-by-item commentary on the Procuring Agency's Technical Requirements, demonstrating the substantial responsiveness of the Information/ TBML System offered to those requirements. In demonstrating responsiveness, the commentary shall include explicit cross references to the relevant pages in the supporting materials included in the bid. Whenever a discrepancy arises between the item-by-item commentary and any catalogs, technical specifications, or other preprinted materials submitted with the bid, the item-by-item commentary shall prevail; c) Preliminary Project Plan describing, among other things, the methods by which the Bidder will carry out its overall management and coordination responsibilities if awarded the Contract, and the human and other resources the Bidder proposes to use. d) The Plan should include a detailed Contract Implementation Schedule in bar chart form, showing the estimated duration, sequence, and interrelationship of all key activities needed to complete the Contract. The Preliminary Project Plan must also address any other topics specified in the BDS. In addition, the Preliminary Project Plan should state the Bidder's assessment of what it expects the Procuring Agency and any other party involved in the implementation of the TBML System to provide during implementation and how the Bidder proposes to coordinate the activities of all involved parties; e) a written confirmation that the Bidder accepts responsibility for the successful integration and inter-operability of all components of the TBML System as required by the Bidding Documents.
14. Form of Bid	14.1	The Bidder shall fill the Form of Bid furnished in the Bidding Documents. The Bid Form must be completed without any alterations to its format and no substitute shall be accepted.

15. Bid Prices	15.1	The Bid Prices and discounts quoted by the Bidder in the Form of Bid and in the Price Schedules shall conform to the requirements specified below in ITB Clause 15 or exclusively mentioned hereafter in the bidding documents.
	15.2	All items in the Schedule of requirement must be listed and priced separately in the Price Schedule(s). If a Price Schedule shows items listed but not priced, their prices shall be construed to be included in the prices of other items.
	15.3	Items not listed in the Price Schedule shall be assumed not to be included in the Bid, and provided that the Bid is still substantially responsive in their absence or due to their nominal nature, the corresponding average price of the respective item(s) of the remaining substantially responsive bidder(s) shall be construed to be the price of those missing item(s): Provided that: where there is only one (substantially) responsive bidder, or where there is provision for alternate proposals and the respective items are not listed in the other bids, the procuring agency may fix the price of missing items in accordance with market survey, and the same shall be considered as final price.
	15.4	The Bid price to be quoted in the Form of Bid in accordance with ITB 15.1 shall be the total price of the Bid, excluding any discounts offered.
	15.5	The Bidder shall indicate on the appropriate Price Schedule, the unit prices (where applicable) and total Bid price of the goods it proposes to deliver under the contract.
	15.6	Prices indicated on the Price Schedule shall be entered separately in the following manner: For goods manufactured from within Pakistan (or within the country where procurement is being done in case of foreign missions abroad): the price of the goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable), including all customs duties and sales and other taxes already paid or payable: on the components and raw material used in the manufacturing or assembly of goods quoted ex- works or ex-factory; or on the previously imported goods of foreign origin quoted ex-warehouse, ex-showroom, or off-the-shelf. all applicable taxes which will be payable on the goods if the contract is awarded. the price for inland transportation, insurance, and other local

		costs incidental to delivery of the goods to their final destination, if specified in the BDS. the price of other (incidental or allied) services, if any, listed in the BDS. For goods offered from abroad: the price of the goods shall be quoted CIF named port of destination, or CIP border point, or CIP named place of destination, in the Procuring Agency's country, as specified in the BDS. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible countries. Similarly, the Bidder may obtain insurance services from any eligible source country. or the price of the goods quoted FOB port of shipment (or FCA, as the case may be), if specified in the BDS. or the price of goods quoted CFR port of destination (or CPT as the case may be), if specified in the BDS. the price for inland transportation, insurance, and other local costs incidental to delivery of the goods from the port of entry to their final destination, if specified in the BDS. the price of (incidental) services, if any, listed in the BDS.
	15.7	Prices proposed on the Price Schedule for goods and related services shall be disaggregated, where appropriate as indicated in this Clause. This desegregation shall be solely for the purpose of facilitating the comparison of Bids by the Procuring Agency. This, shall not in any way limit the Procuring Agency's right to contract on any of the terms and conditions offered: - For Goods: - i. the price of the Goods, quoted as per applicable INCOTERMS as specified in the BDS ii. all customs duties, sales tax, and other taxes applicable on goods or on the components and raw materials used in their manufacture or assembly, if the contract is awarded to the Bidder, and For Related Services i. The price of the related services, and ii. All customs duties, sales tax and other taxes applicable in Pakistan, paid or payable, on the related services, if the contract is awarded to the Bidder.

	15.8	Prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and not subject to variation on any account. A Bid submitted with an adjustable price will be treated as non-responsive and shall be rejected, pursuant to ITB 29.
	15.9	If so indicated in the Invitation to Bids and Instructions to Bidders, that Bids are being invited for individual contracts (Lots) or for any combination of contracts (packages), Bidders wishing to offer any price reduction for the award of more than one contract shall specify in their Bid the price reductions applicable to each package, or alternatively, to individual contracts (Lots) within a package.
16. Bid Currencies	16.1	Prices shall be quoted in the following currencies: For goods and services that the Bidder will deliver from within Pakistan, the prices shall be quoted in Pakistani Rupees, unless otherwise specified in the BDS. For goods and related services that the Bidder will deliver from outside Pakistan, or for imported parts or components of goods and related services originating outside Pakistan, the Bid prices shall be quoted in any freely convertible currency of another country.
	16.2	For the purposes of comparison of bids quoted in different currencies, the price shall be converted into a single currency specified in the bidding documents. The rate of exchange shall be the selling rate, prevailing on the date of opening of (financial part of) bids specified in the bidding documents, as notified by the State Bank of Pakistan on that day.
	16.3	The Currency of the Contract shall be Pakistani Rupee unless otherwise stated in the BDS.
17. Bid Validity Period	17.1	Bids shall remain valid for the period specified in the BDS after the Bid submission deadline prescribed by the Procuring Agency. A Bid valid for a shorter period shall be rejected by the Procuring Agency as non- responsive. The period of Bid validity will be determined from the complementary bid securing instrument i.e., the expiry period of bid security or bid securing declaration as the case may be.
	17.2	Under exceptional circumstances, prior to the expiration of the initial Bid validity period, the Procuring Agency may request the Bidders' consent to an extension of the period of validity of their Bids only once, for the period not more than the period of initial bid validity. The request and the Bidders responses shall be

		made in writing or in electronic forms that provide record of the content of communication. The Bid Security provided under ITB 18 shall also be suitably extended. A Bidder may refuse the request without forfeiting its Bid security or causing to be executed its Bid Securing Declaration. A Bidder agreeing to the request will not be required nor permitted to modify its Bid, but will be required to extend the validity of its Bid Security or Bid Securing Declaration for the period of the extension, and in compliance with ITB 18 in all respects.
	17.3	If the award is delayed by a period exceeding sixty (60) days beyond the expiry of the initial Bid validity period, the contract price may be adjusted by a factor specified in the request for extension. However, the Bid evaluation shall be based on the already quoted Bid Price without taking into consideration on the above correction.
18. Bid Security or Bid Securing Declaration	18.1	Pursuant to ITB 11, unless otherwise specified in the BDS, the Bidder shall furnish as part of its Bid, a Bid Security in form of fixed amount not exceeding five percent of the estimated value of procurement determined by the procuring agency and in the amount and currency specified in the BDS or Bid Securing Declaration as specified in the BDS in the format provided in Section VI (Standard Forms).
	18.2	The Bid Security or Bid Securing Declaration is required to protect the Procuring Agency against the risk of Bidder's conduct which would warrant the security's forfeiture, pursuant to ITB 18.9.
	18.3	The Bid Security shall be denominated in the local currency or in another freely convertible currency, and it shall be in the form specified in the BDS which shall be in any of the following: a bank guarantee, an irrevocable letter of credit issued by a Scheduled bank in the form provided in the Bidding Documents or another form acceptable to the Procuring Agency and valid for twenty-eight (28) days beyond the end of the validity of the Bid. This shall also apply if the period for Bid Validity is extended. In either case, the form must include the complete name of the Bidder; a cashier's or certified cheque; or another security if indicated in the BDS
	18.4	The Bid Security or Bid Securing Declaration shall be in accordance with the Form of the Bid Security or Bid Securing Declaration included in Section VI (Standard Forms) or another form approved by the Procuring Agency prior to the Bid submission.

	18.5	The Bid Security shall be payable promptly upon written demand by the Procuring Agency in case any of the conditions listed in ITB 18.9 are invoked.
	18.6	Any Bid not accompanied by a Bid Security or Bid Securing Declaration in accordance with ITB 18.1 or 18.3 shall be rejected by the Procuring Agency as non-responsive, pursuant to ITB 29.
	18.7	Unsuccessful Bidders' Bid Security will be discharged or returned as promptly as possible, however in no case later than thirty (30) days after the expiration of the period of Bid Validity prescribed by the Procuring Agency pursuant to ITB 17. The Procuring Agency shall make no claim to the amount of the Bid Security, and shall promptly return the Bid Security document, after whichever of the following that occurs earliest: the expiry of the Bid Security; the entry into force of a procurement contract and the provision of a performance security (or guarantee), for the performance of the contract if such a security (or guarantee), is required by the Biding documents; the rejection by the Procuring Agency of all Bids; the withdrawal of the Bid prior to the deadline for the submission of Bids, unless the Biding documents stipulate that no such withdrawal is permitted.
	18.8	The successful Bidder's Bid Security will be discharged upon the Bidder signing the contract pursuant to ITB 42, or furnishing the performance guarantee, pursuant to ITB 43.
	18.9	The Bid Security may be forfeited or the Bid Securing Declaration executed: if a Bidder: withdraws its Bid during the period of Bid Validity as specified by the Procuring Agency, and referred by the bidder on the Form of Bid except as provided for in ITB 17.2; or does not accept the correction of errors pursuant to ITB 31.2; or in the case of a successful Bidder, if the Bidder fails: to sign the contract in accordance with ITB 42; or to furnish performance security (or guarantee) in accordance with ITB 43.
19. Alternative Bids by Bidders	19.1	Bidders shall submit offers that comply with the requirements of the Bidding Documents, including the basic Bidder's technical design as indicated in the specifications and Schedule of

		Requirements. Alternatives will not be considered, unless specifically allowed for in the BDS. If so allowed, ITB 19.2 shall prevail.
	19.2	When alternative schedule for supply and installation of TBML System is explicitly invited, a statement of that effect will be included in the BDS as will the method for evaluating different schedule for TBML System.
	19.3	If so allowed in the BDS, Bidders wishing to offer technical alternatives to the requirements of the Bidding Documents must also submit a Bid that complies with the requirements of the Bidding Documents, including the basic technical design as indicated in the specifications. In addition to submitting the basic Bid, the Bidder shall provide all information necessary for a complete evaluation of the alternative by the Procuring Agency, including technical specifications, breakdown of prices, and other relevant details. Only the technical alternatives, if any, of the Most Advantageous Bidder conforming to the basic technical requirements (without altering the bid price) shall be considered by the Procuring Agency.
20. Withdrawal, Substitution, and Modification of Bids	20.1	Before bid submission deadline, any bidder may withdraw, substitute, or modify its Bid after it has been submitted by sending a written notice, duly signed by an authorized representative, and the corresponding substitution or modification must accompany the respective written notice.
	20.2	Bids requested to be withdrawn in accordance with ITB 20.1 shall be returned unopened to the Bidders.
21. Format and Signing of Bid	21.1	The Bidder shall prepare an original and the number of copies of the Bid as indicated in the BDS, clearly marking each "ORIGINAL" and "COPY," as appropriate. In the event of any discrepancy between them, the original shall prevail: Provided that except in Single Stage One Envelope Procedure, the Bid shall include only the copies of technical proposal.
	21.2	The original and the copy or copies of the Bid shall be typed or written in indelible ink and shall be signed by the Bidder or a person or persons duly authorized to sign on behalf of the Bidder. This authorization shall consist of a written confirmation as specified in the BDS and shall be attached to the Bid. The name and position held by each person signing the authorization must be typed or printed below the signature. All pages of the Bid, except for un-amended printed literature, shall be initialed by the person or persons signing the Bid.

	21.3	Any interlineations, erasures, or overwriting shall be valid only if they are signed by the person or persons signing the Bidder.

SUBMISSION OF BIDS

22. Sealing and Marking of Bids	22.1	In case of Single Stage One Envelope Procedure, the Bidder shall seal the original and each copy of the Bid in separate envelopes, duly marking the envelopes as "ORIGINAL" and "COPY." The envelopes shall then be sealed in an outer envelope securely sealed in such a manner that opening and resealing cannot be achieved undetected. Note: *The envelopes shall be sealed and marked in accordance with the bidding procedure adopted as referred in Rule-36 of PPR-2004.*
	22.2	The inner and outer envelopes shall: be addressed to the Procuring Agency at the address given in the BDS; and bear the title of the subject procurement or Project name, as the case may be as indicated in the BDS, the Invitation to Bids (ITB) title and number indicated in the BDS, and a statement: "DO NOT OPEN BEFORE," to be completed with the time and the date specified in the BDS, pursuant to ITB 23.1.
	22.3	In case of Single Stage Two Envelope Procedure, The Bid shall comprise two envelopes submitted simultaneously, one called the Technical Proposal and the other Financial Proposal. Both envelopes to be enclosed together in an outer single envelope called the Bid. Each Bidder shall submit his bid as under: Bidder shall submit his TECHNICAL PROPOSAL and FINANCIAL PROPOSAL in separate inner envelopes and enclosed in a single outer envelope. ORIGINAL and each copy of the Bid shall be separately sealed and put in separate envelopes and marked as such. c) (c) The envelopes containing the ORIGINAL and copies will be put in one sealed envelope and addressed / identified as given in Sub-Clause 21.2.
	22.4	The inner and outer envelopes shall: be addressed to the Procuring Agency at the address provided in the Bidding Data; bear the name and identification number of the contract as defined in the Bidding Data; and provide a warning not to open before the time and date for bid opening, as specified in the Bidding Data. pursuant to ITB 23.1. In addition to the identification required in Sub- Clause 21.2 hereof, the inner envelope shall indicate the name and address of

		the bidder to enable the bid to be returned unopened in case it is declared "late" pursuant to Clause IB.24 If all envelopes are not sealed and marked as required by ITB 22.2, ITB 22.3 and ITB 22.4 or incorrectly marked, the Procuring Agency will assume no responsibility for the misplacement or premature opening of Bid.
23. Deadline for Submission of Bids	23.1	Bids shall be received by the Procuring Agency no later than the date and time specified in the BDS.
	23.2	The Procuring Agency may, in exceptional circumstances and at its discretion, extend the deadline for the submission of Bids by amending the Bidding Documents in accordance with ITB 9, in which case all rights and obligations of the Procuring Agency and Bidders previously subject to the deadline will thereafter be subject to the new deadline.
24. Late Bids	24.1	The Procuring Agency shall not consider for evaluation any Bid that arrives after the deadline for submission of Bids, in accordance with ITB 23.
	24.2	Any Bid received by the Procuring Agency after the deadline for submission of Bids shall be declared late, recorded, rejected and returned unopened to the Bidder.
25. Withdrawal, Substitution, and Modification of Bids	25.1	A Bidder may withdraw, substitute, or modify its bid after submission, provided that written notice of the withdrawal, substitution, or modification is received by the Procuring Agency prior to the deadline prescribed for bid submission. All notices must be duly signed by an authorized representative and shall include a copy of the authorization (the power of attorney).
	25.2	The Bidder modification, substitution or withdrawal notice shall be prepared, sealed, marked, and dispatched in accordance with the provisions of ITB Clauses 21 and 22 with the outer and inner envelopes additionally marked "MODIFICATION", "SUBSTITUTION" OR "WITHDRAWAL" as appropriate. The notice may also be sent by electronic, telex and facsimile, but followed by a signed confirmation copy, postmarked no later than the deadline for submission of Bids.
	25.3	Bids may only be modified by withdrawal of the original Bids and submission of a replacement Bid in accordance with sub-Clause 25.1. Modifications submitted in any other way shall not be taken into account in the evaluation of Bids.
	25.4	Bidders may only offer discounts to or otherwise modify the prices of their Bids by substituting Bid modifications in accordance with this clause or included in the original bid submission.
	25.5	No Bid may be withdrawn, replaced or modified in the interval between the deadline for submission of Bids and the expiration of

		the period of Bid validity specified by the Bidder on the Form of Bid. Withdrawal of a Bid during this interval shall result in the Bidders forfeiture of its Bid Security or execution of the Bid Securing Declaration.
	25.6	Revised bid may be submitted after the withdrawal of the original bid in accordance with the provisions referred in ITB 25.

OPENING AND EVALUATION OF BIDS

26. Opening of Bids	26.1	The Procuring Agency will open all Bids, in public, in the presence of Bidders' or their representatives who choose to attend, and other parties with a legitimate interest in the Bid proceedings at the place, on the date and at the time, specified in the BDS. The Bidders' representatives present shall sign a register as proof of their attendance.
	26.2	First, envelopes marked "WITHDRAWAL" shall be opened and read out and the envelope with the corresponding bid shall not be opened, but returned to the Bidder. No bid withdrawal shall be permitted unless the corresponding Withdrawal Notice contains a valid authorization to request the withdrawal and is read out at bid opening.
	26.3	Second, outer envelopes marked "SUBSTITUTION" shall be opened. The inner envelopes containing the Substitution Bid shall be exchanged for the corresponding Original Bid being substituted, which is to be returned to the Bidder unopened. No envelope shall be substituted unless the corresponding Substitution Notice contains a valid authorization to request the substitution and is read out and recorded at bid opening.
	26.4	Next, outer envelopes marked "MODIFICATION" shall be opened. No Technical Proposal and/or Financial Proposal shall be modified unless the corresponding Modification Notice contains a valid authorization to request the modification and is read out and recorded at the opening of the Bids. Any Modification shall be read out along with the Original Bid except in case of Single Stage Two Envelope Procedure where only the Technical Proposal, both Original as well as Modification, are to be opened, read out, and recorded at the opening. Financial Proposal, both Original and Modification, will remain unopened till the prescribed financial bid opening date.
	26.5	Other envelopes holding the Bids shall be opened one at a time, in case of Single Stage One Envelope Procedure, the Bidders names, the Bid prices, the total amount of each Bid and of any alternative Bid (if alternatives have been requested or permitted), any discounts, the presence or absence of Bid Security, Bid Securing Declaration and

		such other details as the Procuring Agency may consider appropriate, will be announced by the Procurement Evaluation Committee.
	26.6	In case of Single Stage Two Envelope Procedure, the Procuring Agency will open the Technical Proposals in public at the address, date and time specified in the BDS in the presence of Bidders` designated representatives who choose to attend and other parties with a legitimate interest in the Bid proceedings. The Financial Proposals will remain unopened and will be held in custody of the Procuring Agency until the specified time of their opening.
	26.7	The envelopes holding the Technical Proposals shall be opened one at a time, and the following read out and recorded: (a) the name of the Bidder; (b) whether there is a modification or substitution; (c) the presence of a Bid Security, if required; and (d) Any other details as the Procuring Agency may consider appropriate.
	26.8	Bids not opened and not read out at the Bid opening shall not be considered further for evaluation, irrespective of the circumstances. In particular, any discount offered by a Bidder which is not read out at Bid opening shall not be considered further.
	26.9	Bidders are advised to send in a representative with the knowledge of the content of the Bid who shall verify the information read out from the submitted documents. Failure to send a representative or to point out any un-read information by the sent Bidder's representative shall indemnify the Procuring Agency against any claim or failure to read out the correct information contained in the Bidder's Bid.
	26.10	No Bid will be rejected at the time of Bid opening except for late Bids which will be returned unopened to the Bidder, pursuant to ITB 24.
	26.11	The Procuring Agency shall prepare minutes of the Bid opening. The record of the Bid opening shall include, as a minimum: the name of the Bidder and whether or not there is a withdrawal, substitution or modification, the Bid price if applicable, including any discounts and alternative offers and the presence or absence of a Bid Security or Bid Securing Declaration.
	26.12	The Bidders' representatives who are present shall be requested to sign on the attendance sheet. The omission of a Bidder's signature on the record shall not invalidate the contents and affect the record. A copy of the record shall be distributed to all the Bidders.
	26.13	A copy of the minutes of the Bid opening shall be furnished to individual Bidders upon request.
	26.14	In case of Single Stage Two Envelop Bidding Procedure, after the evaluation and approval of technical proposal the procuring agency, shall at a time within the bid validity period, publicly open the financial proposals of the technically accepted bids only. The financial proposal of bids found technically non-responsive shall be returned un-opened to the respective bidders subject to redress of

		the grievances from all tiers of grievances.
27. Confidentiality	27.1	Information relating to the examination, clarification, evaluation and comparison of Bids and recommendation of contract award shall not be disclosed to Bidders or any other persons not officially concerned with such process until the time of the announcement of the respective evaluation report.
	27.2	Any effort by a Bidder to influence the Procuring Agency processing of Bids or award decisions may result in the rejection of its Bid.
	27.3	Notwithstanding ITB 27.2 from the time of Bid opening to the time of contract award, if any Bidder wishes to contact the Procuring Agency on any matter related to the Bidding process, it should do so in writing or in electronic forms that provides record of the content of communication.
28. Clarification of Bids	28.1	To assist in the examination, evaluation and comparison of Bids of the Bidders, the Procuring Agency may, ask any Bidder for a clarification. Any clarification submitted by a Bidder that is not in response to a request by the Procuring Agency shall not be considered.
	28.2	The request for clarification and the response shall be in writing or in electronic forms that provide record of the content of communication. In case of Single Stage Two Envelope Procedure, no change in the prices or substance of the Bid shall be sought, offered, or permitted, whereas in case of Single Stage One Envelope Procedure, only the correction of arithmetic errors discovered by the Procuring Agency in the evaluation of Bids should be sought in accordance with ITB 31.
	28.3	The alteration or modification in THE BID which in any affect the following parameters will be considered as a change in the substance of a bid: a) evaluation & qualification criteria; b) required scope of work or specifications; c) all securities requirements; d) tax requirements; e) terms and conditions of bidding documents. f) change in the ranking of the bidder
	28.4	From the time of Bid opening to the time of Contract award if any Bidder wishes to contact the Procuring Agency on any matter related to the Bid it should do so in writing or in electronic forms that provide record of the content of communication.

29. Preliminary Examination of Bids	29.1	Prior to the detailed evaluation of Bids, the Procuring Agency will determine whether each Bid: a) meets the eligibility criteria defined in ITB 3 and ITB 4; b) has been prepared as per the format and contents defined by the Procuring Agency in the Bidding Documents; c) has been properly signed; d) is accompanied by the required securities; and e) is substantially responsive to the requirements of the Bidding Documents. The Procuring Agency's determination of a Bid's responsiveness will be based on the contents of the Bid itself.
	29.2	A substantially responsive Bid is one which conforms to all the terms, conditions, and specifications of the Bidding Documents, without material deviation or reservation. A material deviation or reservation is one that: - a) affects in any substantial way the scope, quality, or performance of the Services; b) limits in any substantial way, inconsistent with the Bidding Documents, the Procuring Agency's rights or the Bidders obligations under the Contract; or c) if rectified, would affect unfairly the competitive position of other Bidders presenting substantially responsive Bids.
	29.3	The Procuring Agency will confirm that the documents and information specified under ITB 11, 12 and 13 have been provided in the Bid. If any of these documents or information is missing, or is not provided in accordance with the Instructions to Bidders, the Bid shall be rejected.
	29.4	The Procuring Agency may waive off any minor informality, nonconformity, or irregularity in a Bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any Bidder. Explanation: A minor informality, non-conformity or irregularity is one that is merely a matter of form and not of substance. It also pertains to some immaterial defect in a Bid or variation of a bid from the exact requirements of the invitation that can be corrected or waived without being prejudicial to other bidders. The defect or variation is immaterial when the effect on quantity, quality, or delivery is negligible when contrasted with the total cost or scope of the supplies or services being acquired. The Procuring Agency either shall give the bidder an opportunity to cure any deficiency resulting from a minor informality or irregularity in a bid or waive the deficiency, whichever is advantageous to the Procuring Agency. Examples of minor informalities or irregularities include failure of a bidder to – (a) Submit the number of copies of signed bids required by the

		invitation; (b) Furnish required information concerning the number of its employees; (c) the firm submitting a bid has formally adopted or authorized, before the date set for opening of bids, the execution of documents by typewritten, printed, or stamped signature and submits evidence of such authorization and the bid carries such a signature.
	29.5	Provided that a Technical Bid is substantially responsive, the Procuring Agency may request the Bidder to submit the necessary information or documentation, within a reasonable period of time, to rectify nonmaterial nonconformities or omissions in the Technical Bid related to documentation requirements. Requesting information or documentation on such nonconformities shall not be related to any such aspect of the technical Proposal linked with the ranking of the bidders. Failure of the Bidder to comply with the request may result in the rejection of its Bid.
	29.6	Provided that a Technical Bid is substantially responsive, the Procuring Agency shall rectify quantifiable nonmaterial nonconformities or omissions related to the Financial Proposal. To this effect, the Bid Price shall be adjusted, for comparison purposes only, to reflect the price of the missing or nonconforming item or component.
	29.7	If a Bid is not substantially responsive, it will be rejected by the Procuring Agency and may not subsequently be evaluated for complete technical responsiveness.
30. Examination of Terms and Conditions; Technical Evaluation	30.1	The Procuring Agency shall examine the Bid to confirm that all terms and conditions specified in the GCC and the SCC have been accepted by the Bidder without any material deviation or reservation.
	30.2	The Procuring Agency shall evaluate the technical aspects of the Bid submitted in accordance with ITB 22, to confirm that all requirements specified in Section V – Schedule of Requirements, Technical Specifications of the Bidding Documents have been met without material deviation or reservation.
	30.3	If after the examination of the terms and conditions and the technical evaluation, the Procuring Agency determines that the Bid is not substantially responsive in accordance with ITB 29, it shall reject the Bid.
31. Correction of Errors	31.1	Bids determined to be substantially responsive will be checked for any arithmetic errors. Errors will be corrected as follows: - if there is a discrepancy between unit prices and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected, unless in

		the opinion of the Procuring Agency there is an obvious misplacement of the decimal point in the unit price, in which the total price as quoted shall govern and the unit price shall be corrected; if there is an error in a total corresponding to the addition or subtraction of sub-totals, the sub-totals shall prevail and the total shall be corrected; and where there is a discrepancy between the amounts in figures and in words, the amount in words will govern. Where there is discrepancy between grand total of price schedule and amount mentioned on the Form of Bid, the amount referred in Price Schedule shall be treated as correct subject to elimination of other errors.
	31.2	The amount stated in the Bid will, be adjusted by the Procuring Agency in accordance with the above procedure for the correction of errors and, with, the concurrence of the Bidder, shall be considered as binding upon the Bidder. If the Bidder does not accept the corrected amount, its Bid will then be rejected, and the Bid Security may be forfeited or the Bid Securing Declaration may be executed in accordance with ITB 18.9.
32. Conversion to Single Currency	32.1	To facilitate evaluation and comparison, the Procuring Agency will convert all Bid prices expressed in the amounts in various currencies in which the Bid prices are payable. For the purposes of comparison of bids quoted in different currencies, the price shall be converted into a single currency specified in the bidding documents. The rate of exchange shall be the selling rate, prevailing on the date of opening of (financial part of) bids specified in the bidding documents, as notified by the State Bank of Pakistan on that day.
	32.2	The currency selected for converting Bid prices to a common base for the purpose of evaluation, along with the source and date of the exchange rate, are specified in the BDS.
33. Evaluation of Bids	33.1	The Procuring Agency shall evaluate and compare only the Bids determined to be substantially responsive, pursuant to ITB 29.
	33.2	In evaluating the Technical Proposal of each Bid, the Procuring Agency shall use the criteria and methodologies listed in the BDS and in terms of Statement of Requirements and Technical Specifications. No other evaluation criteria or methodologies shall be permitted.
	33.2	The Procuring Agency's evaluation of a Bid will take into account: in the case of goods manufactured in Pakistan or goods of foreign origin already imported in Pakistan, Income Tax, General Sales Tax and other similar/applicable taxes, which will be payable on the goods if a contract is awarded to the Bidder; in the case of goods of foreign origin offered from abroad, customs duties and other similar import taxes which will be payable on the goods if the contract is awarded to the Bidder; and

	33.3	The comparison shall be between the EXW price of the goods offered from within Pakistan, such price to include all costs, as well as duties and taxes paid or payable on components and raw material incorporated or to be incorporated in the goods, and named port of destination, border point, or named place of destination) in accordance with applicable INCOTERM in the price of the goods offered from outside Pakistan.
	33.4	In evaluating the Bidders, the evaluation committee will, in addition to the Bid price quoted in accordance with ITB 15.1, take account of one or more of the following factors as specified in the BDS, and quantified in ITB 32.5: Cost of inland transportation, insurance, and other costs within the Pakistan incidental to delivery of the goods to their final destination. delivery schedule offered in the Bid; deviations in payment schedule from that specified in the Special Conditions of Contract; the cost of components, mandatory spare parts, and service; the availability (in Pakistan) of spare parts and after-sales services for the equipment offered in the Bid; the projected operating and maintenance costs during the life of the equipment; the performance and productivity of the equipment offered; and/or other specific criteria indicated in the TBS and/or in the Technical Specifications.
	33.5	For factors retained in BDS, pursuant to ITB 33.4 one or more of the following quantification methods will be applied, as detailed in the BDS: a) *Inland transportation from EXW/port of entry/border point, Insurance and incidentals.* Inland transportation, insurance, and other incidental costs for delivery of the goods from EXW/port of entry/border point to Project Site named in the BDS will be computed for each Bid by the PA on the basis of published tariffs by the rail or road transport agencies, insurance companies, and/or other appropriate sources. To facilitate such computation, Bidder shall furnish in its Bid the estimated dimensions and shipping weight and the approximate EXW or as per applicable INCOTERM value of each package. The above cost will be added by the Procuring Agency to EXW or as per applicable INCOTERM price.
		b) *Delivery schedule.* i. The Procuring Agency requires that the goods under the Invitation for Bids shall be delivered (shipped) at the time

		specified in the Schedule of Requirements. The estimated time of arrival of the goods at the Project Site will be calculated for each Bid after allowing for reasonable international and inland transportation time. Treating the Bid resulting in such time of arrival as the base, a delivery "adjustment" will be calculated for other Bids by applying a percentage, specified in the BDS, of the EXW or as per applicable INCOTERM price for each week of delay beyond the base, and this will be added to the Bid price for evaluation. No credit shall be given to early delivery.
		Or ii. The goods covered under this invitation are required to be delivered (shipped) within an acceptable range of weeks specified in the Schedule of Requirement. No credit will be given to earlier deliveries, and Bids offering delivery beyond this range will be treated as non- responsive. Within this acceptable range, an adjustment per week, as specified in the BDS, will be added for evaluation to the Bid price of Bids offering deliveries later than the earliest delivery period specified in the Schedule of Requirements. Or iii. The goods covered under this invitation are required to be delivered (shipped) in partial shipments, as specified in the Schedule of Requirements. Bids offering deliveries earlier or later than the specified deliveries will be adjusted in the evaluation by adding to the Bid price a factor equal to a percentage, specified in the BDS, of EXW or as per applicable INCOTERM price per week of variation from the specified delivery schedule. *c) Deviation in payment schedule.* i. Bidders shall state their Bid price for the payment schedule outlined in the SCC. Bids will be evaluated on the basis of this base price. Bidders are, however, permitted to state an alternative payment schedule and indicate the reduction in Bid price they wish to offer for such alternative payment schedule. The Procuring Agency may consider the alternative payment schedule offered by the selected Bidder. Or ii. The SCC stipulates the payment schedule offered by the Procuring Agency. If a Bid deviates from the schedule and if such deviation is considered acceptable to the Procuring Agency, the Bid will be evaluated by calculating interest earned for any earlier payments involved in the terms outlined in the Bid as compared with those stipulated in this invitation, at the rate per

		annum specified in the BDS.
		d) Cost of spare parts a) The list of items and quantities of major assemblies, components, and selected spare parts, likely to be required during the initial period of operation specified in the BDS, is annexed to the Technical Specifications. The total cost of these items, at the unit prices quoted in each Bid, will be added to the Bid price. Or b) The Procuring Agency will draw up a list of high-usage and high-value items of components and spare parts, along with estimated quantities of usage in the initial period of operation specified in the BDS. The total cost of these items and quantities will be computed from spare parts unit prices submitted by the Bidder and added to the Bid price. Or c) The Procuring Agency will estimate the cost of spare parts usage in the initial period of operation specified in the BDS, based on information furnished by each Bidder, as well as on past experience of the Procuring Agency or other Procuring Agency's in similar situations. Such costs shall be added to the Bid price for evaluation. *e) Spare parts and after sales service facilities in Pakistan* The cost to the Procuring Agency of establishing the minimum service facilities and parts inventories, as outlined in the BDS or elsewhere in the Bidding Documents, if quoted separately, shall be added to the Bid price. *f) Operating and maintenance costs* Since the operating and maintenance costs of the goods under procurement form a major part of the life cycle cost of the equipment, these costs will be evaluated in accordance with the criteria specified in the BDS or in the Technical Specifications. *g) Performance and productivity of the equipment.* i. Bidders shall state the guaranteed performance or efficiency in response to the Technical Specification. For each drop in the performance or efficiency below the norm of 100, an adjustment for an amount specified in the BDS will be added to the Bid Price, representing the capitalized cost of additional operating costs over the life of the plant, using the methodology specified in the BDS or in the Technical Specifications.

		Or ii. Goods offered shall have a minimum productivity specified under the relevant provision in the Technical Specifications to be considered responsive. Evaluation shall be based on the cost per unit of the actual productivity of goods offered in the Bid, and adjustment will be added to the Bid price using the methodology specified in the BDS or in the Technical Specifications.
		(h) *Specific additional criteria.* Other specific additional criteria to be considered in the evaluation and the evaluation method shall be detailed in the BDS and/or the Technical Specifications.
	33.6	If these Bidding Documents allow Bidders to quote separate prices for different Lots, and the award to a single Bidder of multiple Lots, the methodology of evaluation to determine the lowest evaluated Lot combinations, including any discounts offered in the Form of Bid, is specified in the BDS.
34. Domestic Preference	34.1	If the BDS so specifies, the Procuring Agency will grant a margin of preference to certain goods in line with the rules, regulations, regulatory guides or instructions issued by the Authority from time to time.
35. Determination of Most Advantageous Bid	35.1	In case where the Procuring Agency adopts the Cost Based Evaluation Technique and, the Bid with the lowest evaluated price from amongst those which are eligible, compliant and substantially responsive shall be the Most Advantageous Bid.
	35.2	The Procuring Agency may adopt the Quality & Cost Based Selection Technique due to the following two reasons: i. Where the Procuring Agency knows about the main features, usage and output of the products; however not clear about the complete features, technical specifications and functionalities of the goods to be procured and requires the bidders to submit their proposals defining those features, specifications and functionalities; or ii. Where the Procuring Agency, in addition to the mandatory requirements and mandatory technical specifications, requires parameters specified in Evaluation Criteria to be evaluated while determining the quality of the goods: In such cases, the Procuring Agency may allocate certain weightage to these factors as a part of Evaluation Criteria, and may determine the

		ranking of the bidders on the basis of combined evaluation in accordance with provisions of Rule 2(1)(h) of PPR-2004.
36. Abnormally Low Financial Proposal	36.1	Where the Bid price is considered to be abnormally low, the Procuring Agency shall perform price analysis either during determination of Most Advantageous Bid or as a part of the post-qualification process. The following process shall apply: a) The Procuring Agency may reject a Bid if the Procuring Agency has determined that the price in combination with other constituent elements of the Bid is abnormally low in relation to the subject matter of the procurement (i.e. scope of the procurement or ancillary services) and raises concerns as to the capability and capacity of the respective Bidder to perform that contract; b) Before rejecting an abnormally low Bid the Procuring Agency shall request the Bidder an explanation of the Bid or of those parts which it considers contribute to the Bid being abnormally low; take account of the evidence provided in response to a request in writing; and subsequently verify the Bid or parts of the Bid being abnormally low; c) The decision of the Procuring Agency to reject a Bid and reasons for the decision shall be recorded in the procurement proceedings and promptly communicated to the Bidder concerned; d) The Procuring Agency shall not incur any liability solely by rejecting abnormally Bid; and e) An abnormally low Bid means, in the light of the Procuring Agency's estimate and of all the Bids submitted, the Bid appears to be abnormally low by not providing a margin for normal levels of profit. Guidance for Procuring Agency: In order to identify the Abnormally Low Bid (ALB) following approaches can be considered to minimize the scope of subjectivity: (i) Comparing the bid price with the cost estimate; (ii) Comparing the bid price with the bids offered by other bidders submitting substantially responsive bids; and (iii) Comparing the bid price with prices paid in similar contracts in the recent past either government- or development partner- funded.
	36.2	The Procuring Agency will determine to its satisfaction whether the Bidder that is selected as having submitted the most advantageous Bid is qualified to perform the contract satisfactorily, in accordance with the criteria listed in ITB 13.3.
	36.3	The determination will take into account the Bidder's financial, technical, and production capabilities. It will be based upon an

		examination of the documentary evidence of the Bidder's qualifications submitted by the Bidder, pursuant to ITB 13.3, as well as such other information as the Procuring Agency deems necessary and appropriate. Factors not included in these Bidding Documents shall not be used in the evaluation of the Bidders' qualifications.
	36.4	Procuring Agency may seek "Certificate for Independent Price Determination" from the Bidder and the results of reference checks may be used in determining award of contract. Explanation: The Certificate shall be furnished by the bidder. The bidder shall certify that the price is determined keeping in view of all the essential aspects such as raw material, its processing, value addition, optimization of resources due to economy of scale, transportation, insurance and margin of profit etc.
	36.5	An affirmative determination will be a prerequisite for award of the contract to the Bidder. A negative determination will result in rejection of the Bidder's Bid, in which event the Procuring Agency will proceed to the next ranked bidder to make a similar determination of that Bidder's capabilities to perform satisfactorily.

AWARD OF CONTRACT

37. Criteria of Award	37.1	Subject to ITB 36 and 38, the Procuring Agency will award the Contract to the Bidder whose Bid has been determined to be substantially responsive to the Bidding Documents and who has been declared as Most Advantageous Bidder, provided that such Bidder has been determined to be: eligible in accordance with the provisions of ITB 3; is determined to be qualified to perform the Contract satisfactorily; and Successful negotiations have been concluded, if any.

38. Negotiations	38.1	Negotiations may be undertaken with the Most Advantageous Bid relating to the following areas: a minor alteration to the technical details of the statement of requirements; reduction of quantities for budgetary reasons, where the reduction is in excess of any provided for in the Biding documents; a minor amendment to the special conditions of Contract; finalizing payment arrangements; delivery arrangements; the methodology for provision of related services; or clarifying details that were not apparent or could not be finalized at the time of Bidding.
	38.2	Where negotiation fails to result into an agreement, the Procuring Agency may invite the next ranked Bidder for negotiations. Where negotiations are commenced with the next ranked Bidder, the Procuring Agency shall not reopen earlier negotiations.
39. Procuring Agency's Right to to reject All Bids	39.1	Notwithstanding ITB 37, the Procuring Agency reserves the right to reject all the bids, and to annul the Bidding process at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders. However, the Authority (i.e. PPRA) may call from the Procuring Agency the justification of those grounds.
	39.2	Notice of the rejection of all Bids shall be given promptly to all Bidders that have submitted Bids.
	39.3	The Procuring Agency shall upon request communicate to any Bidder the grounds for its rejection of its Bids, but is not required to justify those grounds.
40. Procuring Agency's Right to Vary Quantities at the Time of Award	40.1	The Procuring Agency reserves the right at the time of contract award to increase or decrease the quantity of goods or related services originally specified in these Bidding Documents (schedule of requirements) provided this does not exceed by the percentage indicated in the BDS, without any change in unit price or other terms and conditions of the Bid and Bidding Documents.
41. Notification of Award	41.1	Prior to the award of contract, the Procuring Agency shall issue a Final Evaluation Report giving justification for acceptance or rejection of the bids.
	41.2	Where no complaints have been lodged, the Bidder whose Bid has been accepted will be notified of the award by the Procuring Agency prior to expiration of the Bid Validity period in writing or electronic forms that provide record of the content of communication. The Letter of Acceptance will state the sum that the Procuring Agency will pay the successful Bidder in consideration for the execution of the scope of works as prescribed by the Contract (hereinafter and in the

		Contract called the "Contract Price).
	41.3	The notification of award will constitute the formation of the Contract, subject to the Bidder furnishing the Performance guarantee in accordance with ITB 43 and signing of the contract in accordance with ITB 42.2.
	41.4	Upon the successful Bidder's furnishing of the performance security guarantee pursuant to ITB 43, the Procuring Agency will promptly notify each unsuccessful Bidder, the name of the successful Bidder and the Contract amount and will discharge the Bid Security or Bid Securing Declaration of the Bidders pursuant to ITB 18.7.
42. Signing of Contract	42.1	Promptly after notification of award, Procuring Agency shall send the successful Bidder the draft agreement, incorporating all terms and conditions as agreed by the parties to the contract.
	42.2	Immediately after the Redressal of grievance by the GRC, and after fulfillment of all condition's precedent of the Contract Form, the successful Bidder and the Procuring Agency shall sign the contract.
	42.3	Where no formal signing of a contract is required, purchase order issued to the bidder shall be construed to be the contract.
43. Performance Security (or Guarantee)	43.1	After the receipt of the Letter of Acceptance, the successful Bidder, within the specified time, shall deliver to the Procuring Agency a Performance proportions of currencies in the Letter of Acceptance and in accordance with the Conditions of Contract. Guarantee in the amount and in the form stipulated in the BDS and SCC, denominated in the type and proportions of currencies in the Letter of Acceptance and in accordance with the Conditions of Contract.
	43.2	If the Performance Security Guarantee is provided by the successful Bidder and it shall be in the form specified in the BDS which shall be in any of the following: certified cheque, cashier's or manager's cheque, or bank draft; irrevocable letter of credit issued by a Scheduled bank or in the case of an irrevocable letter of credit issued by a foreign bank, the letter shall be confirmed or authenticated by a Scheduled bank; bank guarantee confirmed by a reputable local bank or, in the case of a successful foreign Bidder, bonded by a foreign bank; or surety bond callable upon demand issued by any reputable surety or insurance company. Any Performance Security (or guarantee) submitted shall be enforceable in Pakistan.
	43.3	Failure of the successful Bidder to comply with the requirement of ITB 43.1 shall constitute sufficient grounds for the annulment of the award and forfeiture of the Bid Security, in which event the Procuring Agency may make the award to the next ranked Bidder or call for new Bids.
44. Advance	44.1	The advance payment will not be provided in normal circumstances.

Payment		However, in case where international incoterms are involved, the same will be dealt with standard international practices and in the manner as prescribed in ITB 44.2.
	44.2	The Procuring Agency will provide an Advance Payment as stipulated in the Conditions of Contract, subject to a maximum amount, as stated in the BDS. The Advance Payment request shall be accompanied by an Advance Payment Guarantee in the form provided in Section IX. For the purpose of receiving the Advance Payment, the Bidder shall make and estimate of, and include in its Bid, the expenses that will be incurred in order to commence Delivery of Goods. These expenses will relate to the purchase of equipment, machinery, materials, and on the engagement of labor during the first month beginning with the date of the Procuring Agency's "Notice to Commence" as specified in the SCC.
45. Arbitrator	45.1	The Arbitrator shall be appointed by mutual consent of the both parties as per the provisions specified in the SCC.
46. Corrupt & Fraudulent Practices	46.1	Procuring Agencies (including beneficiaries of Government funded projects and procurement) as well as Bidders/Suppliers/Contractors under Government financed contracts, observe the highest standard of ethics during the procurement and execution of such contracts, and will avoid to engage in any corrupt and fraudulent practices.

GRIEVANCE REDRESSAL & COMPLAINT REVIEW MECHANISM

47. Constitution of Grievance Redressal	47.1	Procuring agency shall constitute a Grievance Redressal Committee (GRC) comprising of odd number of persons with proper power and authorization to address the complaint. The GRC shall not have any of the members of Procurement Evaluation Committee. The committee must have one subject specialist depending the nature of the procurement.
48. GRC Procedure	48.1	Any party can file its written complaint against the eligibility parameters or any other terms and conditions prescribed in the prequalification or bidding documents found contrary to provision of Procurement Regulatory Framework, and the same shall be addressed by the GRC well before the bid submission deadline.
	48.2	Any Bidder feeling aggrieved by any act of the procuring agency after the submission of his bid may lodge a written complaint concerning his grievances not later than seven days of the announcement of technical evaluation report and five days after issuance of final evaluation report.
	48.3	In case, the complaint is filed against the technical evaluation report, the GRC shall suspend the procurement proceedings.

	48.4	In case, the complaint is filed after the issuance of the final evaluation report, the complainant cannot raise any objection on technical evaluation of the report: Provided that the complainant may raise the objection on any part of the final evaluation report in case where single stage one envelop bidding procedure is adopted.
	48.5	The GRC, in both the cases shall investigate and decide upon the complaint within ten days of its receipt.
	48.6	Any bidder or the procuring agency not satisfied with the decision of the GRC may file Appeal before the Appellate Committee of the Authority on prescribed format after depositing the Prescribed fee.
	48.7	The Committee, upon receipt of the Appeal against the decision of the GRC complete in all respect shall serve notices in writing upon all the parties to appeal.
	48.8	The committee shall call the record from the concerned procuring agency or the GRC as the case may be, and the same shall be provided within prescribed time.
	48.9	The committee may after examination of the relevant record and hearing all the concerned parties, shall decide the complaint within fifteen (15) days of receipt of the Appeal.
	48.10	The decision of the Committee shall be in writing and shall be signed by the Head and each Member of the Committee. The decision of the committee shall be final.

MECHANISM OF BLACKLISTING

49. Mechanism of Blacklisting	49.1	The Procuring Agency shall bar for not more than the time prescribed in Rule-19 of the Public Procurement Rules, 2004, from participating in their respective procurement proceedings, bidder or contractor who either: Involved in corrupt and fraudulent practices as defined in Rule-2 of Public Procurement Rules; Fails to perform his contractual obligations; and Fails to abide by the id securing declaration;
	49.2	The show cause notice shall contain: (a) precise allegation, against the bidder or contractor; (b) the maximum period for which the Procuring Agency proposes to debar the bidder or contractor from participating in any public procurement of the Procuring Agency; and (c) the statement, if needed, about the intention of the Procuring Agency to make a request to the Authority for debarring the bidder or contractor from participating in public

		procurements of all the procuring agencies.
	49.3	The procuring agency shall give minimum of seven days to the bidder or contractor for submission of written reply of the show cause notice
	49.4	In case, the bidder or contractor fails to submit written reply within the requisite time, the Procuring Agency may issue notice for personal hearing to the bidder or contractor/ authorize representative of the bidder or contractor and the procuring agency shall decide the matter on the basis of available record and personal hearing, if availed.
	49.5	In case the bidder or contractor submits written reply of the show cause notice, the Procuring Agency may decide to file the matter or direct issuance of a notice to the bidder or contractor for personal hearing.
	49.6	The Procuring Agency shall give minimum of seven days to the bidder or contractor for appearance before the specified officer of the Procuring Agency for personal hearing. The specified officer shall decide the matter on the basis of the available record and personal hearing of the bidder or contractor, if availed
	49.7	The procuring Agency shall decide the matter within fifteen days from the date of personal hearing unless the personal hearing is adjourned to a next date and in such an eventuality, the period of personal hearing shall be reckoned from the last date of personal hearing.
	49.8	The Procuring Agency shall communicate to the bidder or contractor the order of debarring the bidder or contractor from participating in any public procurement with a statement that the bidder or contractor may, within thirty days, prefer a representation against the order before the Authority.
	49.9	Such blacklisting or barring action shall be communicated by the procuring agency to the Authority and respective bidder or bidders in the form of decision containing the grounds for such action. The same shall be publicized by the Authority after examining the record whether the procedure defined in blacklisting and debarment mechanism has been adhered to by the procuring agency.
	49.10	The bidder may file the review petition before the Review Petition Committee Authority within thirty days of communication of such blacklisting or barring action after depositing the prescribed fee and in accordance with “Procedure of filing and disposal of review petition under Rule-19(3) Regulations, 2021”. The Committee shall evaluate the case and decide within ninety days of filing of review petition
	49.11	The committee shall serve a notice in writing upon all respondent of the review petition. The notices shall be accompanied by the copies

		of review petition and all attached documents of the review petition including the decision of the procuring agency. The parties may file written statements along with essential documents in support of their contentions. The Committee may pass such order on the representation may deem fit.
	49.12	The Authority on the basis of decision made by the committee either may debar a bidder or contractor from participating in any public procurement process of all or some of the procuring agencies for such period as the deemed appropriate or acquit the bidder from the allegations. The decision of the Authority shall be final.

SECTION III: BID DATA SHEET (BDS)

A. Bid Data Sheet (BDS)

The following specific data for the TBML System to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITBs). Whenever there is a conflict, the provisions herein shall prevail over those in ITBs.

BDS Clause Number	ITB Number	Amendments of, and Supplements to, Clauses in the Instruction to Bidders
A. Introduction		
1.	1.1	Name of Procuring Agency: National Bank of Pakistan (NBP). The Description (as specified in IFB) of the System is: **TRADE BASED MONEY LAUNDERING SYSTEM** Period for delivery: Please refer delivery schedule in Section V – Delivery Schedule Commencement date for delivery: Please refer delivery schedule in Section V – Delivery Schedule
2.	2.1 & 2.2	Financial year for the operations of the Procuring Agency: 2025 Name of Project **TRADE BASED MONEY LAUNDERING SYSTEM**
3.	3.1	Joint Venture is not applicable.
4.	4.6	Demonstration of authorization by manufacturer: Required

B. Bidding Documents

5.	7.2	The required documents shall be uploaded on EPADS.
6.	8.1	All the clarifications and their responses shall be made through EPADS.
	8.5	Pre-bid meeting will be held [*Y*] If yes write down the venue, time, and date of the pre-Bid meeting: Date time: XX-MMM, 2025, at Divisional Head Procurement Venue: Procurement Division, Logistics, Communications & Marketing Group, National Bank of Pakistan, 3rd Floor, Head Office Building, Karachi. 021-99220331, 021-38902647

C. Preparation of Bids

7.	10.1	The Language of all correspondences and documents related to the Bid is: ENGLISH
8.	11.1 (h)	In addition to the documents state in ITB 11, the following documents must be included with the Bid All technical product documents mentioned in Section V
9.	12.3 (c)	Other procurement specific documentation requirements are: [*As per the technical requirement document for evidence of mandatory technical requirements*].
10.	12.4	Spare parts required for 03 of years of operation.
11.	13.3 (b)	The qualification criteria required from Bidders in ITB 13.3(b) is modified as follows: Please refer to the section V The Bidder is required to include with its Bid, documentation from the manufacturer of the TBML System, that it has been duly authorized to deliver, in Pakistan, the TBML System indicated in its Bid.
12.	15.6 (a)	For goods making TBML Systems manufactured from within Pakistan the price quoted shall ONLY be in PKR (Pakistani Rupee)
13.	15.6 (a) (i) & 15.6 (b)	For goods offered from abroad the price quoted shall be*:* *[PKR/USD], in case the price is quoted in more than one currency, PKR cost will be considered as the quoted price for final evaluation and award of contract.*
14.	15.8	The price shall be fixed for the duration of the contract. No additional cost will be borne by the bank. (FIXED PRICE CONTRACT)
15.	16.1 (a)	a) For TBML System originating in Pakistan the currency of the Bid shall be *Pakistani Rupees*; b) For Information System originating outside Pakistan, the

		Bidder shall express its Bid in any convertible currency.
16.	16.2	For the purposes of comparison of bids quoted in different currencies, the price shall be converted into a single currency specified in the bidding documents. The currency that shall be used for Bid evaluation and comparison purposes to convert all Bid prices expressed in various currencies is: PKR The source of exchange rate shall be: The selling rate prevailing on the date of opening of the financial bids intimated by NBP, as notified by the State Bank of Pakistan NBP Exchange rate of the date of opening will be used for evaluation.
17.	17.1	The Bid Validity period shall be *180* days.
18.	18.1	The amount of Bid Security shall be: PKR 1,000,000/- The currency of the Bid Security shall be in Pakistani Rupees [PKR].
19.	18.3	The Bid Security shall be in the form of: Bank Guarantee. Form of Bid Security (Bank Guarantee) is provided in Section – VI Standard Form.
20.	18.3 (c)	Other forms of security are:[NIL]
21.	19.1	Alternative Bids to the requirements of the Bidding Documents will not be permitted.
22.	21.1	The number of copies of the Bid to be completed and returned shall be *01.*
23.	21.2	Written confirmation of authorization are: *Letter of authorization to sign contract & Submit proposal on behalf of bidding company signed by CEO or board resolution.*

D. Submission of Bids

24.	22.2 (a)	Bid shall be uploaded on EPADS.
25.	22.2 (b)	Title of the subject Procurement or Project name: **TRADE BASED MONEY LAUNDERING SYSTEM** ITB title and No: Please refer websites (NBP & PPRA) Time and date for submission XX-MMM , 2025

26.	23.1	The deadline for Bid submission is a) Day *:* _____ *b)* Date*: XX-MMM-2025* c) *Time:* _____

E. Opening and Evaluation of Bids

27.	26.1	The Bid opening shall take place at EPADS.
28.	32.2	The currency that shall be used for Bid evaluation and comparison purposes to convert all Bid prices expressed in various currencies is: *PKR* The source of exchange rate shall be: *The selling rate prevailing on the date of opening of the financial bids intimated by NBP, as notified by the State Bank of Pakistan NBP Exchange rate of the date of opening will be used for evaluation.*
29.	33.4 (h)	Other specific criteria are [*as per the detailed Technical and Payment section*]
30.	33.5 (a)	Inland transportation from EXW/port of entry/border point to NBP Datacenter HO Building and DR Site, and insurance and incidentals. Please refer to bidder criteria in section V
31.	33.5 (b)	Delivery schedule. Please refer to delivery schedule in section V
32.	33.5 (c) (ii)	Deviation in payment schedule is not applicable.

33.	33.5 (d)	Cost of spare parts. *Please refer to section V BOQ*
34.	33.5(e)	Spare parts and after sales service facilities in Pakistan. *Please refer to section V BOQ*
35.	33.5 (f)	Operating and maintenance costs. Factors for calculation of the whole life cost: *Please refer to section V BOQ*
36.	33.5 (g)	Performance and productivity of TBML System. *Please refer to the Technical Requirement Section V*
37.	33.5 (h)	Specific additional criteria to be used in the evaluation and their evaluation method *Please refer to section V BOQ*, Technical Specification and Bidder criteria, Delivery Schedule and Payments terms.
38.	33.6	In case of award to a single Bidder of multiple lots; the methodology of evaluation to determine the lowest evaluated Lot combinations, including any discounts offered in the Form of Bid is elaborated in evaluation criteria laid out in Section V
39.	34.1	a) Domestic preference to apply. Preference to domestic or national suppliers or contractors shall be provided in accordance with policies of the Federal Government and/or in accordance with the regulations issued by the Authority.
40.	35	Evaluation Techniques Quality and Cost Based Selection (QCBS) In such combination, there shall be some specific weightage of both the technical features (such as prescribed in ITB 35.2) and financial aspects of the proposal. The financial marks shall be awarded on the basis of inverse proportion calculations. The highest ranked bid shall be declared, on the basis of combined evaluation. Please refer to evaluation criteria laid out Section V – Evaluation Criteria, Qualification Criteria and Technical Evaluation

Note:
For the purposes of this tender, NBP has used the Standard Bidding Documents provided for TBML System by Public Procurement Regulatory Authority. However, all reference to manual processes and manual submission of tender should be deemed to have been replaced with the processes and procedures defined in E-PAK Procurement Regulation, 2023. Any query in this regard may be made to Divisional Head Procurement, LCMG – National Bank of Pakistan on haider.isani@nbp.com.pk

F. Award of Contract

41.	40.1	Percentage for quantity increase or decrease is Not applicable, however please refer to section V
42.	43.1	The Performance Security (Guarantee) shall be 10% of the total quoted amount of the qualified bidder.
43.	43.2	The Performance Guarantee shall be in the form of Bank Guarantee.
44.	44.2	Maximum amount of Advance payment shall be 10% against advance bank guarantee, please refer to section V payment plan
45.	45.1	Arbitrator shall be appointed by mutual consent of the both parties.

G. Review of Procurement Decisions

46.	48.1	The address of the Procuring Agency Procurement Division, Logistics, Communications & Marketing Group, National Bank of Pakistan 3rd Floor, Head Office Building, Karachi
47.	48.6	The Address of PPRA to submit a copy of grievance: Grievance Redressal Appellate Committee, Public Procurement Regulatory Authority 1st Floor, G-5/2, Islamabad, Pakistan Tel: +92-51-9202254

Section IV. Eligible Countries

All the bidders are allowed to participate in the subject procurement without regard to nationality, except bidders of some nationality, prohibited in accordance with policy of the Federal Government.

Following countries are ineligible to participate in the procurement process:

1. India
2. Israel

Ministry of Interior, Government of Pakistan has notified List of Business-Friendly Countries (BVL). information can be accessed through following link:

http://www.dgip.gov.pk/Files/Visa%20Categories.aspx#L

SECTION V: SCHEDULE OF REQUIREMENTS, TECHNICAL SPECIFICATION

I. Evaluation Criteria

The bids/proposals with all complete documents will be evaluated as under:

1) All bidders are required to submit filled, correct and complete Technical Requirement Document along with their bids. If the bidder fails to do so, its bid will be considered as rejected. All bidders are also requested to affix their company's stamp/signature on each page of the submitted Technical Requirement Document.

2) All bidders are required to propose single solution for **TRADE BASED MONEY LAUNDERING SYSTEM** as per the requirements of NBP as any alternate or additional Solution will not be considered for evaluation and such bid will be deemed as rejected.

3) For evaluation of solution requirements mentioned in Technical Requirement, NBP will request bidders to demonstrate their proposed software to NBP (if required) during evaluation stage, at no extra cost to NBP. The place, date & time of demonstration sessions will be communicated to bidders separately by NBP. If any bidder failed to demonstrate its respective solution, its bid will be considered as technically disqualified / rejected / non-responsive.

4) For evaluation of requirements mentioned under Section V (Technical Specification), bidder is required to provide undertaking on company's letterhead signed by authorized representative of the company mentioning all the requirements and also stating that all requirement in RFP are acceptable to the company and will be provided to NBP accordingly. NBP will first check that such undertaking has been provided or not in the submitted bid. If undertaking is not found then NBP will ask clarification from the bidder and ask to submit the required undertaking, however if bidder failed to provide the correct and complete undertaking then its bid will be considered as rejected.

5) All the bidders are required to submit technical architecture and technical requirement of proposed solution for **TRADE BASED MONEY LAUNDERING SYSTEM**.

6) NBP may ask any other additional documentary evidence or explanation against any item for clarification that must be provided by the Bidder during the period of evaluation. Bidders should respond to such requests within the time frame indicated in the correspondence (letter/fax/ e-mail). If the bidder fails to provide the required information within given timeframe, its bid will be considered as rejected.

7) Technical Requirements mentioned in Technical Requirement Document with "Priority (High/Low)" is evaluated as follows:

   a) For evaluation purpose, a desired response of only 'Y', 'Yes', 'N', 'No' is required in the availability column for all technical requirements (mentioned in Technical Requirement Document).

b) All technical requirements with "High" Priority must be answered as 'Y'/'Yes' or 'N'/'No'. If bidder response 'N'/'No' against any of such "High" Priority requirement, its bid will be considered as technically disqualified and will be rejected.

c) For with "Low" Priority can be answered as 'Y'/'Yes', 'N'/ 'No'. If bidder responds 'N' or 'No' or 'blank' against any of the "Low" Priority requirement, its bid will not be rejected.

d) For all requirements against which Bidder is not providing any response (i.e. an empty availability cell or an availability cell with a response other than ''Y'/'Yes' or 'N'/'No'), NBP will first check that against such requirements proper reference documents have been provided or not in the submitted bid. If reference document is found then NBP ask clarification from the bidder about its response, however if reference document will also not found or provided then response of bidder shall be considered as 'No' and its bid will be considered as rejected if the requirement item is high priority.

e) For all "High" priority technical requirements against which Bidder is responding "Y", all bidders are required to provide Documentation with proper reference (Section No/ Page No) in the proposal against all requirements. It is mandatory to provide proper reference of document. It is NBP's discretion to raise clarification queries against requirements where reference is provided, and further clarification is required. Incase no reference is available, and documents are not available in the submitted proposal, NBP may not raise any clarification query and response will be considered as NIL, which may lead to disqualification.

f) For all "Low" priority technical requirements against which Bidder is responding "Y", all bidders are required to provide Documentation with proper reference (Section No/ Page No) in the proposal against all requirements. It is mandatory to provide proper reference of document. It is NBP's discretion to raise clarification queries against requirements where reference is provided, and further clarification is required. Incase no reference is available, and documents are not available in the submitted proposal, NBP may not raise any clarification query and response will be considered as NIL.

g) Bidder must mention Y-Yes or N-No or C-Customizable in 'Availability Response Column' for all the 'Requirements' mentioned in this document as Low or High Priority. The 'N' mentioned for High Priority item will disqualify the bidder. The 'C' mentioned for High Priority Item will presume that customization is covered in given cost and within the given timelines. [The Bidder may provide 'C' (Customization required) only against requirements mentioned in "Technical Requirements", which should not exceed 30% of those requirements.] If bidder responses of 'C' against these 'High' Priority requirements become greater than 30%, its bid will be considered as technically disqualified / rejected / non-responsive. The C- Customizable mentioned for Low Priority Items will be presumed available upon submitting a change request (CR) by NBP whilst N-No mentioned for Low Priority Item will reflect not possible and may not impact on merit of solution.

h) All bidders are required to submit the proposals with proper page numbering with master table of contents of all attached documents in the proposal.

8) The bidders are required to include the price of all requirements with 'High' priority where the response is 'Y' in its financial proposal as the price mentioned in financial proposal will be considered as final and cannot be increased in any case after the submission of bid.

9) "Low" priority requirements that shall be responded "Y" by bidder shall be treated as complimentary, without any addition in the above-mentioned quoted price.

10) Financial proposals will be opened for only technically qualified bidders. Technically unqualified bidders will be considered as disqualified and their financial proposals will be returned un-opened.

11) The Bidders must include price of all requirements with its Financial Proposal as the price mentioned in Financial Proposal will be considered as final and cannot be changed in any circumstances after the submission of bid.

12) The prices will be evaluated on the basis of all items mentioned under Section V Technical Requirement and BOQ of the RFP documents which will be considered as total bid value/ bid amount / contract price.

13) As per requirement of ITB 31 mentioned in Section VI – Standard Form of RFP, NBP may conduct a post-qualification evaluation exercise for the bidder which is selected as having submitted the lowest evaluated bid. A negative evaluation will result in rejection of the bidder's bid, in which event NBP shall proceed to the next lowest evaluated bidder to make a similar evaluation.

14) Combined evaluation of technical and financial proposals shall follow and the bidder with the winning proposal will be accepted (i.e. the proposal that will obtain maximum marks will be considered as the "Lowest Evaluated Bid" and will be accepted for contract award.)

II. BOQ – Bill of Quantity

Item(s)	Quantity
Licenses o f Complete Proposed Solution as mentioned in Technical Requirements. (If any)	Minimum 30 Licenses will be required for Trade Operations Team, Compliance Team & Risk Management Team
Installable Media for complete solution (Executable Code for all Modules as mentioned under Section V Technical Specification).	2 copies
Project Management, Requirement Analysis, Designing, Development / Customization, Implementation, System Integration Testing (SIT) and User Acceptance Testing (UAT), Training, Go-Live, Support etc.	As required throughout contract period
Users (Functional + Technical) Training of Proposed System for NBP's employees.(With multiple training sessions)	Up to 10 persons (Technical) Up to 100 persons (Functional)
Product Complete Technical & User level documentation (For example; Software Requirement Specifications, Design Document, Database ERD, Installation Guide, User Manual, Train the Trainer Manual etc.)	2 Sets (Soft & Hard Copies)
Options of Escrow services for Source code should be available (this will also be part of contract)	To be arranged by the vendor
Complete TBML Solution Software Support and Maintenance Including troubleshooting, Technical Support, Bug Fixing, release/version upgrades (Major and Minor), patches after Go-Live date of complete solution and On-Site Post-Implementation Support.	06 months
On-Site Post-Implementation Support After Go-Live	06 months

Note:

The bidder is required to thoroughly examine the Technical Requirements and may add any missing items to the above Bill of Quantities (BOQ) in relation with Technical Requirements.

III. Delivery Schedule

Bidder must propose the Project Timelines in accordance with the Delivery Schedule mentioned below:

Description	Required Delivery from the date of signing of contract	Location
Project Initiation Phase	Within 15 days	
Project Implementation Phase Project Implementation duration including all Customization required to fulfill all requirements mentioned in Technical Requirements using Agile Methodology. (Requirement Analysis, Designing, Development / Customization, Implementation, Training and User Acceptance Testing along with content creation requirement as per technical annexure).	Within 6 Months	NBP Head office, Karachi
Operational / Go-Live date of Complete Solution	Within 2 Month after completion of Project.	
On-site Post Implementation Support	06 Months after Go- Live date of complete Solution.	

Support & Maintenance including, troubleshooting, technical Support, Bug Fixing, Release Upgrades, Software Patches, etc. Proposed Solution Software Support & Maintenance Agreement including Release Upgrades, Software Update(s), Bug/Issues fixing, Patches, etc. after Go-Live and On-Site Post-Implementation Support.	Three Year after Go-Live and on-site post implementation support Date and after completion of On-site post implementation support period.	

IV. Payment Terms / Plan

Price Schedule

Price Schedule mentioned in Standard Bidding Section has been modified and Bidders are required to provide the total bid amount / price with their bid as per following table in its financial proposal considering all items mentioned in Technical Requirements and BOQ document.

Item(s)	Amount (in PKR)
The below details should be given for each module of TBML System	
Installation of module – On premises – One time cost (if any)	
Annual Subscription Cost (if any)	
Integration Cost with Allied Systems (if any)	
Software License Cost for NBP Users (if any)	
Bidder must provide details on fully transferable license with one-time initial cost to NBP, irrespective of employees and local and overseas locations. In case there is any licensing cost based on users, the bidder is required to provide details with the proposed solution and annual support cost if any. Bidder should provide an undertaking that the solution must be equipped to manage up multiple users (minimum 30 licenses) (within NBP, or its overseas operations)	
Cost of Professional Services (Project Management, Requirement Analysis, Designing, Development / Customization, Implementation, Data Migration, Training, On-Site Post-Implementation Support for 06 Months after Go-Live etc.)	
Application Support and Maintenance services	
Cost of 1st year software support & maintenance after Go-Live & after Completion of six months' onsite Post Implementation support period.	

Cost of 2nd year software support & maintenance. Cost of 3rd year software support & maintenance.	
Total Bid Amount (i.e. Total Contract Price) in PKR	

Note: In case of discrepancy between unit and total price, the unit price shall prevail. The prices should include the price of incidental services. No separate payment shall be made for the incidental services. Financial Evaluation will be based on the sum / total of all prices in above-mentioned Price Schedule, which will be the Total Bid Amount / Contract Price.

1) Cost of 1st year software support & maintenance will be valid for next two (02) years upon renewal of Support & Maintenance Agreement.

2) Total Bid amount must be inclusive of all applicable taxes.

3) Bidders shall quote all prices in Pakistani Rupees (PKR) only. If any bidder quotes the bid prices other than Pak Rupees, the interbank conversion rate in Pak Rupees (as determined by NBP) on the day of financial bid opening will be considered for calculating total bid amount in Pakistani Rupees (PKR) and for evaluating of their bids.
4) In case the price is quoted in PKR as well as in other currency, then the PKR price will be considered for the evaluation of the bid.

5) If the bid price is quoted in more than one currency (e.g. PKR with equivalent USD amount), then NBP shall only consider the bid price quoted in PKR in the proposal for evaluation purposes.

6) NBP will make all payments in Pakistani Rupees (PKR) only.

7) Within 60 calendar days after the signing of the contract, successful bidder is required to submit a Performance Security which shall be ten (10%) percent of the total bid amount / Contract Price. The Performance Security shall be in the form of a "Bank Guarantee" only from the reputable bank of Pakistan. The performance security amount shall be in Pakistani Rupees (PKR). The contract will only be considered effective after submission and verification of "Bank Guarantee" by the contractor. In case the contractor fails to submit the "Bank Guarantee" in 28 calendar days, his Bid security will be forfeited and the contract will be terminated.

8) Discharge of the Performance Security shall take place; after thirty (30) days of completion of 3-month post-implementation warranty / support period (support and maintenance after Go-Live). Submission of incomplete Performance Guarantee and/or fake Bank Guarantee will lead to immediate disqualification of successful bidder and NBP will pursue to blacklist the company as per Public Procurement Rules, 2004.

Payment Schedule for Software Licenses & Professional Services

No.	Payment Milestones	Total Cost of Professional Services Cost (in %age)
1.	Project Initiation Phase: Project team mobilization, submission of detailed Project Plan. Analysis Phase: Initial assessment, user requirement gathering and Delivery of 02 (two) sets of Software Requirement Specifications. Certificate of "Acceptance of Software Requirement Specifications" from NBP is required along with the invoice for payment.	10
2.	Designing Phase: System designing as per outcome of Analysis Phase. Delivery of 02 (two) sets of Software Design Document & Database ERD etc. Development Phase: Development / Customization / Data Migration (if required), Delivery of Software Licenses, configuration and customization of solution according to NBP requirements and provide Training to NBP Teams on final developed system. Delivery of 02 (two) sets of User Manual, Train the Trainer Manual, Desktop Instructions Manual etc.	10
3.	System Integration Testing (SIT): Certificate of "Successful completion of SIT Phase" from NBP's representative is required along with the invoice for payment.	10
4.	User Acceptance Testing (UAT) Phase: Sign Off on UAT test scripts and installation of solution in the UAT environment. Certificate of "Successful completion of User Acceptance Testing Phase" from NBP's representative is required along with the invoice for payment.	20
5	Deployment & Go-Live Phase: Implementation of UAT finalized software on Production/DR environment.	30
6	Post Go Live: Certificate of "Completion of 6 Months Post-Implementation after successful Go Live" from NBP's representative is required along with the invoice for payment.	20

Payment Schedule for Application Hosting, Support & Maintenance for 3 Years

Total annual cost of Application Hosting, Support & Maintenance shall be paid in one installment. The installment will be paid at the start of each year to the bidder after receipt of invoice from bidder. The cost of first year Hosting, Support and Maintenance will be submitted by bidder as mentioned above in price schedule, the same annual cost will be valid for next two years upon renewal. Bidder should

submit the renewal request for 'Support / license &Maintenance Contract' along with invoice of 'Support / license & Maintenance' cost f o r 2nd and 3rd years.

Payment Schedule for Software and License Support & Maintenance for 3 Years

Total annual cost of Software and license Support & Maintenance shall be paid in one installment. The installment will be paid at the start of each year to the bidder after receipt of invoice from bidder. The cost of first year Support and Maintenance will be submitted by bidder as mentioned above in price schedule, the same annual maintenance cost will be valid for next two years upon renewal. Bidder should submit the renewal request for 'Support / license & Maintenance Contract' along with invoice of 'Support / license & Maintenance' cost for 2nd and 3rd years.

Note: All payments are subject to adjustment for any non-delivery or compromised delivery of committed feature mentioned in RFP or non-satisfactorily support & maintenance services during the contract period. The formula for this deduction/adjustment will be agreed between NBP and successful bidder at the time of signing of contract / SLA.

V. Qualification Criteria

S.No.	Qualification Criteria	Priority (High/Low)
1	BIDDER QUALIFICATION & SYSTEM REQUIREMENTS	
1.1	Bidder Qualification Requirement	
1.1.1	Bidder must be registered with Income Tax and Sales Tax Departments and should provide a copy of valid NTN/STN and Active Tax Payer Certificate.	High
1.1.2	Bidder should provide certificate of incorporation or ordinance of the organization or university, with any proof of being in this business for at least two (02) years.	High
1.1.3	Bidders must have a documented track of at least two (2) live implementations locally or globally of "Trade Based Money Laundering System" and providing Maintenance and Technical support as the direct authorized agent / dealer / partner of the manufacturer in Pakistan. Bidder must provide Reference Letters / Purchase / Work Orders from the customers where the solution is deployed and last implementation details.	High
1.1.4	The bidders must have verifiable presence/support/branch office in Pakistan.	High
	Bidder must provide audited Profit & Loss (Income Statement) showing Sale volume of company of at least Rs.50 Million in each last 3 years. If audited statement is not available for last year then Bidder	

1.1.5	should provide letter from company's CFO or senior management staff confirming that Sale Volume of company was at least Rs.50 Million in last year. Audited Financial Statements of last 02 Years of the Company / Bidder shall be provided in case of Limited Company (Private/Public). For Partnership concern, Financial Statements of last 03 Years duly signed by the relevant authorities of the Company / Bidder shall be provided.	High
1.1.6	Bidder must provide an undertaking on non-judicial stamp paper of 500 Rupees stating that "the bidder's company is not blacklisted by any Government entity in Pakistan for unsatisfactory past performance, corrupt, fraudulent or any other unethical business practices and also not involved in any kind of lawsuits either current or pending." (The undertaking on legal paper provided by the bidder must cover all points in the statement mentioned above).	High
1.1.7	Bidder must have a dedicated team in Pakistan that can customize and integrate the platform as per NBP's current and future requirements.	High
1.1.8	Bidder must provide 03 (three) CV's/Profile of their proposed implementation and configuration team which should be employees of the company since last one year and must have relevant experience for proposed solution.	High
1.1.9	Bidder must have Direct Partnership with the principal supplier and also must provide "Manufacturer Authorization Form / Authorized Partner / Distribution Certificate" from principal supplier as per the requirements (guarantee, warranty and maintenance etc.) stated in the specimen attached under Section VI - Standard Form. Kindly note that exact statements mentioned in the specimen are not required, however, NBP requirements of (guarantee, warranty and maintenance etc.) shall be explicitly covered. Bidders must be a manufacturer or an authorized agent/dealer/partner of the manufacturer in Pakistan with a currently valid authorization certificate of Principal.	High
1.1.10	Bidder must provide undertaking that the proposed solution is an international or national level solution. The bidder must also confirm therein that he is content specialist for the proposed solution.	High
1.1.11	Bidder must not be sole proprietor but a proper Pvt. limited registered firm with at least 15-20 number of staff members or some Govt. body, institution or academic body/ university.	High
1.1.12	Bidder must provide the responses on SSDLC checklist and fulfill ISD requirement.	High

1.1.13	Bidder must be CMMI Level 3 or above compliant or have other equivalent certifications.	Low
1.1.14	Bidder must provide Solution architecture diagram and technical requirement of proposed solution.	High

Note:

1) *Bidder must mention Y-Yes or N-No or C-Customizable in 'Availability Response Column' for all the 'Requirements' mentioned in this document as Low or High Priority. The 'N' mentioned for High Priority item will disqualify the bidder.*

2) *The 'C' mentioned for High Priority Item will presume that customization is covered in given cost and within timelines.*

3) *The Bidder may provide 'C' (Customization required) only against requirements mentioned from 1.20 to 4.4.10 in "Technical Requirements", which should not exceed 30% of those requirements.*

4) *If bidder responses of 'C' against these 'High' Priority requirements become greater than 30%, its bid will be considered as technically disqualified / rejected / non-responsive.*

5) *The C- Customizable mentioned for Low Priority Items will be presumed available upon submitting a change request (CR) by NBP.*

6) *N-No mentioned for Low Priority Item will reflect not possible and may not impact on merit of solution.*

VI. Technical Specification

National Bank of Pakistan
Procurement of Trade Based Money Laundering System
Technical Requirements
Tender ID:
Note: All participating bidders are advised to thoroughly review Evaluation Criteria before providing their responses against below mentioned requirements.

S.No.	Technical Requirement	Priority (High/Low)	Availability Response (Yes/No)	Bidder Response and/or proposal Reference (Section/Page No.)
A	TRADE BASED MONEY LAUNDERING SYSTEM			
1.	General Requirements			
1.1	Vendor will perform business analysis and customize the software in order to capture relevant requirements and all details necessary for the design of the required solution as per State Bank of Pakistan Framework for Managing Risks of Trade Based Money Laundering and Terrorist Financing issued in 2019, SBP Framework for TBML is here under: Including but not limited to the following: • Implementation of required modules with all features and controls to meet regulatory requirement and minimum human interaction and intervention. . • The vendor shall provide plan on training, tutoring, including comprehensive training contents and share all mandatory material to business users and IT Staff including but not limited to provisioning of user manual and administrative guide. • Timely solution to the problem through on-site visit.	High		
1.2	The Vendor will ensure smooth implementation of Trade Based Money Laundering System so that the day-to-day activities of Trade Operations, Compliance and Risk	High		

	Management function will continue uninterrupted.			
1.3	Vendor shall implement the following module for NBP TBML system : 1. Price Due Diligence 2. Vessel Tracking 3. Container Tracking 4. Dual Use Goods 5. TBML Scenarios 6. Trade Documents Validation 7. MIS & Dashboards 8. Integration with Bank Systems Each Module should have "Help Option" display for each item with description. Video Tutorial/training material tab on each module.	High		
1.4	System must be capable of providing reports for audit trail with time and date stamp.	High		
1.5	System must be complied with SSDLC checklist (refer: Annexure I) provided by bank's information Security Division(ISD) for Bidder Qualification and Technical Requirements. Bidder also need to complied any new requirement by SBP or NBP ISD during implementation/Go-Live.	High		
1.6	In case of cloud based solution, compliance with SBP regulations should be mandatory. (refer: Annexure II)	High		
1.7	Upon selection of bidder, Functional specification document (FSD) with complete architecture diagram with respect to NBP environment (including communication protocol, authentication mechanism, integration with other components like TI, etc.) should be provided before deployment phase.	High		
2.	Regulation Assessment, Maintenance & Updation			
2.1	The vendor shall ensure that the system shall have a process to identify and upgrade the system as per new/ evolving regulatory requirements without additional cost.	High		
3.	Price Due Diligence			
3.1	The system shall be capable of evaluating the deviation in pricing between the amount/ value of underline goods/ commodity input in the system based on shipping documents and the prices available on multiple reliable resources which includes but not limited to FBR, PSW, WEBOC, OGRA, Platts of all regions, shipping line data, TDAP, websites, historical	High		

	appraisement etc. on real time basis in terms of percentage and absolute value as defined in the SBP Framework on TBML issued in 2019.			
3.6	The system shall maintain and update the following list - List of goods which are exempt from import-related duties. - list of goods which are subject to over 25% import-related duties This data should be used by system in evaluating price variance.	High		
3.9	The system shall have capability to validate HS code , unit of measure & custom duty against the product description	High		
3.10	The system shall be capable to give alert if the deviation in the price is more than given threshold as per bank policy and subject to change whenever required.	High		
3.11	The system shall be capable to evaluate the deviation all the components of price including but not limited to Unit Price (FoB), Freight & other components like premium etc. Each product has different components of pricing which should be catered accordingly.	Low		
3.13	The system shall be capable to generated report with complete details with Time and date stamp for audit trail purpose.	High		
4	Vessel Tracking			
4.1	The system shall be capable to provide vessel Information which includes but not limited to Name. AIS Name, IMO number, Country, Country ISO, Type, Year Built, Weigh & Size, Home port, European Number of Identification etc.	High		
4,2	The system shall be capable to provide vessel position on real time basis and tracking record which includes but not limited to Last Position, Last Position Date, Region, Nearest Port and its distance, Departure Port, Destination Port, Actual time of Departure, estimated time of arrival, details of instance in case vessel had touched or come close to any sanction port/ country/ vessel, details of instance in case vessel had switched off transponder in past etc.	High		
4.3	The system shall be capable to provide vessel Ownership which includes but not limited to Cover Flag, Owner, Manager, Operator, Technical Manager, insurer etc.	High		
4.10	The system shall be capable to verify the Bill of Lading	High		

4.11	The system shall be capable to generate the report with date and time stamp for audit trail.	High		
5	Container Tracking			
5.1	The system shall be capable to provide container information which includes but not limited to type, number, status, sealine name, ISO Code, AT, Transshipment, Sanction country, departure port, Arrival port, Discharge port and IMO, Vessel Flag of vessel in which it is placed etc.	High		
5.2	The system shall be capable to search container through various information like Container number, booking number and its tracking and navigation details should be provided by system.	High		
5.3	The system shall be capable to provide mapping on real time basis and historical tracking record	High		
5.4	The system shall be capable to Track containers events like Empty to shipper, arrival at first port of loading, loading and discharge at transshipment (T/S) ports, vessel departure and arrival etc.	Low		
6	Dual Use Goods			
6.1	The system shall be capable to identify whether a specific product is subject to import and export control regulation.	High		
6.2	The system shall be capable to identify/ detect the underline Good as Dual Use Good by using information like Product Name, CAS number, HS Code, category, sub-category, serial number etc.	High		
6.3	The system shall be capable to update the list of Dual Use Goods as per latest regulatory changes.	High		
6.4	The system shall be capable to over complete range of Dual Use Goods by using different list including but not limited to following; - Sec Div - Wassenaar - United States Commerce Control List - United Kingdom Strategic Control List	High		
7	TBML Scenarios			
7.1	The system shall be capable to detect Red Flags in the transactions on Pre-check and Post-Check basis.	High		
7.2	The system shall have comprehensive list of TBML Red Flags including but not limited to Red Flags given by SBP & FMU in their Regulations respectively.	High		
7.5	The system shall have option of Case Management of Alerts.	Low		
7.6	The system shall have ability to update the Red Flags are the latest guideline, regulations and industry practice.	High		

7.7	The system shall have capability to maintain historical records of Red Flags, alerts, scenarios, cases and system changes.	High		
8	Trade Documents Validation			
8.1	The system shall be capable to match GD declared value with the payment against import/ export bills and generate alert in case of deviation.	High		
8.2	The system shall be capable to detect deviations between GD declared v/s assessed value	High		
8.3	The system shall be capable to detect deviation between FIs details and GDs.	Low		
8.4	The system shall be capable to detect duplication of Invoices, Goods Declaration, Transport Documents already used	High		
9	MIS & Dashboards			
9.1	The system shall be capable to generated meaningful MIS by using available information to give end to end view of trade portfolio and audit trail.	High		
9.2	The system shall be capable to formulate different Dashboards to analyze trade data, monitor compliance and extract valuable insight for historical analysis and status updates.	High		
9.3	The system shall be capable to generate reports of non-performance and overdue status of import payments and export receipts respectively to meet regulatory requirements.	High		
10	Integration with Bank Systems			
10.1	The system shall be capable to integrate with existing bank system including but not limited to Trade Application (TI+), Account Opening System (AOS), Core Banking System (CBA) for smooth data exchange and process automation.	High		
10.2	The system shall restrict duplicate data entry by automating data capture and synchronization across systems through real time connectivity.	High		
11	Access and Control			
11.1	The system shall be capable to implement robust controls to ensure security and confidentiality	High		
11.2	The system shall be capable to define user roles, assign permissions as per department/role.	High		
11.3	System shall not use built-in super admin ID to run systems operations for routine tasks.	High		
11.4	System should be capable to assign limited administrative authority to named authorized application administrators.	High		
11.5	System shall be capable of integration with the SIEM solution for information security at NBP.	HIGH		
12	Performance			

12.1	Ability to perform at or above specifications. Fast as possible with acceptable performance in regions with poor internet performance.	High		
12.2	System must support multiple users. (Minimum 30 concurrent users)	High		
13	Support			
13.1	Support through multiple mediums. (E.g. Email, fax, telephone, chat, helpdesk portal with ticketing system, etc.) Bidder should have 24x7x365 Corporate Helpline availability for reporting and resolution of all kinds of issues and escalations via including Phone Support, Email Support or Online customer portal to access support tickets for escalation and resolution	High		
13.2	Bidder must provide complaint reporting and escalation matrix and/or software solution for NBP to report any issue / complaint and its rectification / resolution in the proposed solution.	High		
13.3	Onsite or Virtual Support within Pakistan should be available.	High		
14.	IMPLEMENTATION AND TESTING REQUIREMENTS			
14.1	Implementation			
14.1.1	Bidder before the start of implementation must provide hardware and software requirement , the entire installation process / implementation guidelines to NBP, including the installations related to application / database / web server etc., in conjunction with all other suppliers and contractors.	High		
14.1.2	Bidder must provide relevant examples/supported by rationale, of previously implemented in similar projects. Examples may include but not limited to strategy and execution plan, production of any digital content, production of any print content, distribution mechanism.	High		
14.1.3	System must support text editor, embed external resources, multimedia integration including video, audio and presentation files.	Low		
14.1.4	Bidder is required to provide the Proof of Concept (POC) of the proposed solution along with the presentation / solution screenshots with the proposal. Presentations / Demo session will be scheduled as per NBP requirements.	High		
14.2	Testing			
14.2.1	Bidder should provide the performance benchmark / metrics of the proposed solution. Note: The bidder would also develop and provide a testing methodology for the provided performance	High		

	benchmark/metrics of the proposed solution, in coordination with NBP, after being awarded the contract. NBP will perform testing (which may not be limited to single test cycle) of complete solution after its deployment and any gaps found therein would be fixed by the bidder without any additional cost.			
14.2.2	Issues / bugs reporting, tracking and resolution tools must be provided to NBP.	High		
15	LICENSE, MAINTENANCE, TRAINING, SECURITY, STABILITY & CONTINUITY			
15.1	License and Maintenance Support			
15.1.1	Bidder must provide an undertaking that it will not bind NBP for any component upgrades (i.e. OS, Software, Database, Reporting tools etc.) during the period of maintenance & support. However, consent on compatibility will be sought from bidder. Latest version of the solution should be implemented and all patched should be included during contract period under SLA. The methodology for implementing new releases / updates of your software should be described along with specifying user notification process, frequency of updates, update media options and the process by which changes are identified to be included in a new release.	High		
15.1.2	Bidder must provide the cost of implementation, maintenance and support & warranty (including license, if applicable) for (01) one year after system implementation and user acceptance testing. This is separate from the SLA Agreement, which shall come into effect after completion of the support service period.	High		
15.1.3	Bidder must provide cost of a support and maintenance (including license, if applicable) of proposed solution for two (02) consecutive years after the date of expiry of 1st year contract period. It is on bank's discretion to opt for 2nd and 3rd year support and maintenance agreement.	High		
15.2	Training			
15.2.1	Bidder must provide comprehensive training (functional + technical) to business as well as IT users of NBP on the proposed solution. Details of high level Training Plan / Schedule should be provided by the Bidder with the proposal.	High		
15.2.2	Bidder must provide undertaking that whenever, there will be new release the bidder will also provide modified desktop manuals, training manuals and user manuals as part of maintenance agreement signed between NBP & Bidder.	High		
	Bidder must provide training sessions for NBP staff as trainers			

15.2.3	and course creators including video-recording and editing of lectures with hands on experience.	High		
15.2.4	Bidder must provide Training Guides, Trainer's guides and Frequently Asked Questions for learners (in both Urdu and English Languages) for the proposed / implemented solution.	High		
15.2.5	Bidder must provide architecture diagram with process flow of application internal and external integration technically and logically with detailed briefing.	High		
15.3	Security			
15.3.1	System must have ability to define new roles and privileges and assign multiple roles and privileges to the users. Services Menu of users on interface should be based on assigned privileges only.	High		
15.3.2	System must support single sign-on to access all granted modules of proposed System i.e. Separate login should not be required to access modules of proposed System individually.	High		
15.3.3	Have capability to disallow multiple concurrent sessions of User-id.	High		
15.3.4	Support automatic log-off or time-out the session after a defined configurable period of time.	High		
15.3.5	Be able to block / unblock any user through centralized user management interface.	High		
15.3.6	Have configuration control for allowed login attempts in a day. Number of failed attempts must be controlled through a parameter.	High		
15.3.7	Have user Password configuration / control parameters which at a minimum include minimum password length -, alphanumeric, auto-reset password (forget password option) / password generation / construction requirements, password change, password expiry period, password change attempts allowed per day, password change on first login, and non-display of password in clear text on any interface / screen.	High		
15.3.8	All passwords must be stored and transferred in encrypted form and never in clear text.	High		
15.3.9	Application must have inputter / authorizer function for all administrative and end-user processes .			
15.3.10	VAPT of application (white box, Black and Grey box penetration testing) by third party is mandatory. Bidder should provide undertaking that it will provide its full support in remediating and fixing all issues that will be reported by ISD and third party company during the Penetration Testing / Ethical Hacking / Web Vulnerability assessment of the proposed System. This exercise will be performed before Go-Live phase.	High		
	System must provide complete audit trail of unauthorized			

15.3.11	access, rejected sign on attempts, authorization level changes, Alert's definition and issuance, etc. Logs should be maintained for user activity, admin activity, user management activity, security, user login attempts etc. as required by Audit	High		
15.3.12	System must provide last access time and date upon login, deployment of content and editing, etc.	High		
15.3.13	System must maintain history of all modifications of roles with date and time stamp and user performing the activity.			
15.3.14	The application server(s) must have support to be exposed on public servers only via authenticated latest versions of SSL/TLS based connections or recommended by banks ISD.	High		
15.3.15	The bidder must ensure that system should be protected against all kind of vulnerabilities including all kind of virus/hacking/phishing attacks (including but not limited to DDoS, MITM, SQLi, XSS, Malware Attacks etc.)	High		
15.3.16	There must be no provision for creation of anonymous accounts within application.	High		
15.3.17	Maker-checker functionality must be available for User Access Management and activities related to Security Parameterization.	High		
15.3.18	Application source code must not be accessible to Administrators.	High		
15.3.19	Administrative accounts must not have access to logs of their own activities.	High		
15.3.20	All default access capabilities (including passwords) must be changeable.	High		
15.3.21	Application must be able to auto disable users not logged in to the system for certain period of days (configurable).	High		
15.3.22	Application system must generate reports for User List, Invalid Login Details with defined Time Duration, Changes in User Rights, 60/90 Day Login Details.	High		
15.3.23	HTTPS protocol must be implemented.	High		
15.3.24	Application time must be synchronized with NTP Server.	High		
15.3.25	Errors should reveal only necessary information without disclosing any internal system detail.	High		
15.3.26	Passwords or keys must not be hardcoded within application.	High		
15.3.27	User credentials must not be cached within application.	High		
15.3.28	Application must not allow creating more than one User ID with same name.	High		
15.3.29	Any modification of user password must be notified to user via registered Email ID.	High		
15.3.30	Adequate input filtering controls must be in place to address SQL injection, XSS, RCE and unauthorized file inclusion threats.	High		

15.3.31	Validations performed at client end must also be performed at server end.	High		
15.3.32	The bidder must apply security patches in line with service level agreement as soon as patches are available for new vulnerabilities disclosed via CVE no. etc. in technologies/systems which are the part of proposed solution's architecture.	High		
15.3.33	User's credentials and private information such as PII & profile details must not be accessible via browser's local storage / session storage after the user logs out from application.	High		
15.3.34	The logging system in proposed solution must have the capability to integrate with standard security monitoring tools/solutions such as SIEM (IBM QRadar, Guardium, Splunk, AlienVault etc.).	High		
15.3.35	The database platform must support password configuration / control parameters for database users, which at a minimum includes: minimum password length (i.e. 8 characters length for standard users and 12 characters for administrative/privilege users), alphanumeric with special characters, failed login attempts, password life and password history.	High		
15.3.36	The database must have capability to enable/generate a comprehensive audit trail, which includes all types of database user's activities/events and provide integration with third party database security and SIEM solutions.	High		
15.3.37	The database platform must have capability to change passwords of default and unused database accounts.	High		
15.3.38	The database should provide best-practice security configuration as per industry leading compliance standards, such as CIS benchmarks etc.	High		
15.3.39	The database platform must provide native capability of data encryption for sensitive data. Database encryption should be flexible to implement on complete database, table space or at column level. In addition, Database should be flexible to support integration with any 3rd party database encryption solutions.	High		
15.3.40	The database must provide native capability of data redaction/masking for sensitive data. In addition, Database should be flexible to support integration with any 3rd party data masking/redaction solutions.	High		
15.3.41	The database must provide role-based-access control at the granular level and allow database administrator to centrally manage roles and privileges of database users.	High		
15.4	Solution Stability and Business Continuity & Contingency			

	Plan- Disaster Recovery Plan			
15.4.1	Escalation process against incident Management , for immediate repair actions in the event of application failure causing an interruption in service. Incident management plan to be provided as well	High		
15.4.2	Availability of releases / patches which are critical for system stability / security.	High		
15.4.3	Bidder must provide full support and manuals to setup Application's disaster recovery site and both Application and Database replication.	High		
15.4.4	Bidder must to assist NBP in connecting the proposed system with the NBP'S Disaster recovery site.	High		
15.4.5	Proposed system must include details / SOPs of back up System and mechanism to switch to disaster recovery site.	High		
15.4.6	System Backup Mechanism must be provided with step-wise procedure document for execution of the same.	High		
15.4.7	Proposed system must include details of set up required for high availability with Active-Active solution.	High		
15.4.8	The System Architecture must be based on the principles of performance, scalability and security.	High		
15.4.9	The System deployment must consider high - availability and DR environment with 99.99% uptime.	High		
15.4.10	If application is version based then proper version management must be available and documented.	High		
15.4.11	The System must be able to support any remote connectivity software chosen by NBP in case remote access is required for any operation.	High		
16	Other Technical Requirement			
16.1	The Proposed Solution must be compatible with, but not limited to, these browsers: Microsoft edge, Google Chrome, and Mozilla Firefox.	High		
16.2	Bidder must provide one solution for Trade Ops, Compliance & Risk Management.	High		
16.3	The Proposed Solution must support latest version of database platforms like Oracle and MS SQL Server. NBP will decide which database to select and proceed.	High		
16.4	The Proposed Solution must 1. Be able to be deployed as Container based and 2. Be able to be hosted on MS Windows and Linux VM and 3. Be able to be hosted on Intel based hardware with latest MS Windows and Linux operating systems. Deployment model will be at NBP's discretion.	High		

Annexure-1: SSDLC Checklist

Bidder to provide response with below options, where appropriate in SSDLC checklist.

1. True
2. False
3. N/A
4. Other (explain)

Application Security Review Checklist (Bidder to provide response)			Availability Response	Bidder Response
INSTRUCTIONS: Fill in all applicable sections.		Guide		
1.0	Application Components	Acceptable Criteria	(Yes/No)	
1.1	Are Application Components identified ?	Identify all application components (either individual or groups of source files, libraries, and/or executables) that are present in the application		
1.2	Are Application Dependencies identified ?	Identify all components that are not part of the application but that the application relies on to operate.		
1.3	Is the Application Architecture Defined ?	Identify a high-level architecture of the application.		
1.4	Are Application Business/Security Functions Identified ?	Identify all application components and defined in terms of the business functions and/or security functions they provide.		
2.0	Identification and Authentication			
2.1	Authentication of End-users Is the authentication mechanism implemented for end users?	If the application contains only public information then user authentication may not be required. A user Authentication mechanism must be implemented if the application contains Confidential, Sensitive Information with PII, Sensitive or Private information. The strength of the authentication mechanism must be commensurate with the risk of the application. e.g. two factor authentication for Customer facing internet applications or digital Certificates.		
2.2	Authentication for Administrator: Is the authentication mechanism implemented for administrator?	An authentication mechanism for Administrator must be implemented for the application regardless of which class of data the application contains. The administrator authentication mechanism must be at least as strong as the user authentication mechanism.		
2.3	Unique ID for user Does the application use a unique login ID for each user?	The generation of login IDs of users must be uniquely identifiable to user. If the answer is "No" it is unacceptable.		

2.4	Error Message for Failed login Attempts Does the application use a generic message for login attempts failures and account lockout?	All authentication controls fail securely. The error message for any failed login attempts and account lockout must be generic to prevent ID/Password guessing attacks. E.g. Invalid ID, Incorrect Password messages are not allowed. Log all authentication decisions. This should include requests with missing required information, needed for security investigations.		
2.5	User ID generation for Customer Are the identities generated based on the non-public information?	User identities should be generated without containing personal data e.g. personal data like ATM/Credit Card number, CNIC number. Email IDs can contain user names.		
2.6	Initial Password Does the application prompt to change the initial password?	Initial password should be pre-expired. Application should immediately prompt to change the initial password after the users first log into the application.		
2.7	Clear Text Password Password is never displayed on the screen in clear text (with the exception of one time use password resets).	All password fields do not echo the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete		
2.8	Static Password Strength Policy If static password are being used for authentication, is the strength policy being enforced to ensure password meets IT Security policy criteria, Password Expiration Notification, Password history, Maximum failed login attempts?	Password parameters shall be configured in accordance to NBP IT Security Policy as mentioned below: Password history should be maintained for at least 10 passwords. Password Should be hard to guess. It should not constitute with the common predict phrases like names, Tel Number, Date of Birth, Anniversary, same as user name etc. Account should be locked after 3-5 consecutive unsuccessful login attempts, release of locked account automatically after 30 minutes is recommended. User Level • Minimum 8 characters • Users should be forced to change on or before the expiry period of 45 days. • Account should be locked after 3-6 unsuccessful login attempts, and should only be unlocked upon receipt of request from valid user to the administrator. Privilege Level • Minimum 11 characters • Privilege / admin users should change their password on or before password expiry policy setting of 90 days.		
2.9	Static Password Rules If static password are being used, are the following password rules enforced? Password should be different from user name Password should not be easily guessable Password should not be blank	The strength of any authentication credentials are sufficient to withstand attacks that are typical of the threats in the deployed environment. Password should be different from user name Password should not be easily guessable passwords e.g. 12345678, asdfasdf, etc. Password should not be blank		

2.10	Session Inactivity Timeout Does the application enforce a session inactivity timeout?	Inactivity timeout for the users should be implemented to prevent unauthorized access of an active login session when the user is not present. Inactivity timeout period should be based on the application IS risk level which may be 5 to 15 minutes.		
2.11	Secure Authentication Protocol Is the application using the authentication based on the international standards	A secure mutual authentication protocol with a proper key management scheme to encrypt credentials (e.g. password) should be used. Examples are Kerberos, TLS. One time password or dynamic password can be sent in the clear over the network.		
2.12	Security Contexts Does the authentication server create unique security contexts for the authenticated users	secure session IDs / secure cookies / Kerberos tickets		
2.13	Dynamic Password System If a Dynamic password (one-time) system is used for authentication, it is approved by the Information Security and relevant stake holders.	All Dynamic password system must be reviewed by the Information Security before implementation.		
2.14	Digital Certificates and Certificate Authority (CA) If digital certificates are used, are they issued by approved CA?	Digital Certificates used by the application should be issued by approved CA authority/certificates provider e.g. VeriSign CA. Self-signed certificates can be used for testing purposes. PGP and point-to-point secure file transfer can be used where endpoint authentication is not required.		
2.15	Biometric Authentication if a Biometric Authentication mechanism is used by the application, is it approved by the IS?	Biometric authentication mechanism tend to be one-off solutions and are driven by business requirements (like ATM Authentication) therefore, they should be reviewed and approved by the IS to ensure they are secure.		
2.16	Two Factor Authentication if a two factor Authentication mechanism is used by the application, is it approved by the IS?	Two factor authentication or MFA should be reviewed by the IS/SME before the implementation.		
2.17	Single Sign-On (SSO) If the internet application is using shared authentication services, is it reviewed and approved by IS?	SSO or any shared authentication services should be reviewed by the IS/SME before the implementation.		
2.18	Logout Does the application allow users to completely log out from the application?	The application must provide the logout capability such that the user can completely log out of the application.		
2.19	Brute Force Attacks Is the resource governor controls in place to protect the application against vertical & horizontal brute forcing attacks?	The resource governor is in place to protect against vertical (a single account tested against all possible passwords) and horizontal brute forcing (all accounts tested with the same password e.g. “Password1”). A correct credential entry should incur no delay. Both these governor mechanisms should be active simultaneously to protect against diagonal and distributed Attacks.		
3.0	Authorization / Access Control /			

	Entitlement			
3.1	Authorization / Access Control / Entitlement If the application contains private or higher data, does the application provide mechanisms to control access based on the identity of the authenticated user.	Access control should be implemented and auditable. Users are given only those privileges necessary to perform their function. e.g. via entitlement profile / group / role base which are based on the Least Privilege. Access controls fail securely.		
3.2	Inactive / Obsolete Entitlement review Does the application support a mechanism to review inactive / obsolete entitlements	To ease entitlement review, it is beneficial if inactive/ obsolete entitlement can shown by the application		
3.3	Entitlement Review report Does the application provides the complete details of all users entitlement in form of a report? Security Administrator should have the ability to generate these reports per department / unit for periodic user entitlement review.	To ease entitlement review, application should generate the complete entitlement report of users for periodic entitlement review. High risk application should be able to provide the fine-grained entitlements. Verify that all access control decisions are being logged and all failed decisions are logged.		
3.4	Functional ID Management Does the application have a defined owner who is responsible for all aspects of the Functional IDs including usage, entitlement review and password management			
3.5	Access Control for Privileged Actions Does the application enforce access control for the following privilege actions? • Create, modify and delete user accounts and groups • Configure passwords or account lockout policy • Change passwords or certificates of user • Establish log sizes, fill threshold and behavior.	Access control on privileged access should be enforced to maintain system integrity. If least privilege cannot be enforced, compensating controls should be implemented to mitigate the risk (e.g. activity log review)		
3.6	Account management functions are account management functions secure.	All account management functions (such as registration, update profile, forgot username, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.		
3.7	Re-Authentication is re-authentication required before any sensitive operations	Re-authentication is required before any application-specific sensitive operations are permitted. E.g. authenticating the customer again when conducting Financial Transaction or creating a beneficiary on an internet facing application		

3.8	Authenticity and Integrity of Authorization Data Is authorization data being stored on the client side (e.g. cookies, tickets) after the users get authenticated? If yes, is any mechanism being implemented to protect authorization data, prevent spoofing and maintain its integrity?	If authorization data is being stored on the client, it is important to ensure authorization data is protected/encrypted against unauthorized modification by the user. Ideally authorization data should be stored on the server to maintain data integrity.		
3.9	File and Directory Protection Is file and directory authorization enabled for user access control?	In addition to user entitlement, file and directory access control lists should be configured properly to protect the application's files against unauthorized access.		
3.10	Remote access System For internal application if non-NBP staff access this application remotely, is it over an approved solution which is reviewed and approved by IS?	All remote access to NBP systems / networks used by non-NBP staff (e.g. vendor) must be reviewed and approved by the IS.		
4.0	Data Confidentiality and Data Integrity			
4.1	Input Validation Does the application validate user inputs? Is input validation performed on the server or Client side?	Web Application that take data input can be exploited by the following attacks: buffer overflow, cross site scripting (XSS), SQL injection, code injection, denial of service and elevation of privileges. Input is validated to check for valid types, formats, lengths, and ranges and to reject invalid input. This validation is more critical if input filenames, URLs or user names are used for security decisions. Input validation must be performed on the server side instead on the client side to prevent it from being bypassed. Input validation should be enforced for the following: • Input from users • Parameter from URLs • Values from Cookies • Hidden fields to prevent SQL injection • Filter out character like single quotes, doNBPe quotes, slashes, back-slashes, semi colons, extended characters like NULL, carry return, new lines, etc. in all strings • Convert a numeric value to an integer or check whether it is an integer before parsing it into an SQL statement.		
4.2	Data Protection in Transit Is the sensitive or above category data protected during transmission in certain specific environments.	Identify the list of sensitive data processed by this application and there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). The transmission of data can take many forms including, but not limited to electronic file transfer (e.g. FTP), web traffic, e-mail, tapes, CDs, DVDs, Disk and so on. Transmission of sensitive PII should be encrypted. All cached or temporary copies of sensitive data are protected from unauthorized access or		

		purged/invalidated after the authorized user accesses.		
4.3	Input length Does the application limit the length of each user input field?	The length of every field should be limited		
4.4	Input Manipulation Does the application prevent Sensitive and above data from being passed in clear ?	Sensitive and above data especially authentication data must not be passed in clear text to prevent it from being manipulated by users.		
4.5	Content Cache Does the application prevent Sensitive and above data from being cached on user's local disk.	Sensitive and above data should not be cached on user's local disk. It could be accomplished in web application by implementation HTTP response header with: 'Prama:No-cach' for ASP or 'Cache-control: No cache' for JSP/Servlet.		
4.6	File Upload If the application supports file upload functionality, does it enforce the following a. Validate file extension/type, and file format. b. Run virus/malware scan on the uploaded file.	If data files are being uploaded to NBP servers from the external entity, the receiving server must have anti virus software to scan files before processing. The controls should be inplace to check the integrity of files such as Hashes. Only process the allowed/agreed file extensions. It is a sound practice to validate file extension / type, file format and run scan on the uploaded files, especially executables or other file type that can carry and propagate viruses.		
4.7	Data Protection in Storage Is data at the sensitive or above category protected in storage?	Sensitive and above category data must be protected/encrypted in storage and only accessible by respective users.		
4.8	Password Protection in Storage Is password data protected in storage	Account passwords are salted using a salt that is unique to each account and hashed before storing. All authentication credentials for accessing services external to the application are encrypted and stored in a protected location (not in source code).		
4.9	PII data Mask If the application has a feature to deliver or display an e-statement for customer account activities or to export production PII data, are customer account number/CNIC/credit card number partially masked?	Any combination of PII (personally Identifiable Information) that identifies an individual human being in a manner that would facilitate identity theft, credit fraud or other financial fraud must be protected against unauthorized access. Customer name or contact information in combination with CNIC number or tax number, passport number or account number is an example of Sensitive PII. Also note that when production data is exported for testing, PII data should be masked.		
5.0	Cryptography & Key Management			

5.1	Cryptographic Keys List all type of cryptographic keys such as symmetric, asymmetric, secure hash keys used in the solution. Describe their use scenarios and the security mechanisms associated with each cryptographic algorithm used	if encryption is used for authentication, data protection, key management, digital signature or other purposes, all cryptographic keys including their type, cryptographic algorithms and key length and secure hash algorithm must be listed as a pre-requisite for key management assessment. For instance, an application may implement 2048-bit RSA digital certificates for user authentication and key management, 128-bit AES for data protection in transit, and SHA-2 for password protection.		
5.2	Cryptographic Algorithms and Key lengths Do all cryptographic keys comply with current market standards/requirements? (AES/3DES/RC4, SHA-2/256, RSA etc.) and key length?	Security of the data encryption shall depend on secrecy of the key, not secrecy of the algorithm. All the cryptographic algorithms and key length being used must be validated against FIPS 140-2 or an equivalent current market standards/requirements, Symmetric keys: 168-bit 3DES, 128 AES Asymmetric keys: 2048-bit RSA or 256-bit ECDSA or ECDH Source hash: SHA2 (i.e. SHA-256/384/512)		
5.3	Key Generation & Management Are all cryptographic keys randomly generated using approved Random Number Generator? What type of random number generator is used by the application?	All cryptographic keys must me randomly generated by approved random number generator (e.g. as per NIST FIPS 140-2), also define how cryptographic keys are managed (e.g., generated, distributed, revoked, expired)		
5.4	Key Data Display if a manual key entry process is used, do utilities used to load or enter keys or key components prevent the display of the data loaded or entered in the clear?	Distribute the key between multiple custodians and prevent to display the keys in clear during entry		
5.5	Key Renewal Frequency Do all cryptographic keys have a defined renewal frequency period to comply with	Cryptographic keys should be changed on a periodic basis commensurate with the frequency of key use or exposure to eavesdropping or unauthorized access. E.g. • Key encryption: At least once per month (automated) • Master keys or symmetric keys for authentication or key management : at least once per year (if manual renewal) • Cryptographic keys that cannot be renewed should have a pre-defined expiration period (e.g. 3 years of PIN generation keys)		
5.6	Key Protection in Storage Are all symmetric and asymmetric (private) keys, except public keys, encrypted and stored in a hardware or software cryptographic module with proper access control?	Cryptographic keys except public keys, must be encrypted in storage with proper access control. Access control must be prevent unauthorized access.		

5.7	Hard-coding Cryptographic Keys Does the application prevent any encryption keys or passkey being included in the source code or configuration files?	• Hard coded keys that are manually set into code or part of the application and cannot be changed are not acceptable as the keys are known to developers and all instances of the application should use the same set of keys. • Cryptographic keys being coded as the default should be configured and changeable during installation or configuration. • if Cryptographic keys are hardcoded they cannot be changed. Therefore, not acceptable.		
5.8	Certification Validation When digital certificates are used for the digital signature or authentication, is an up-to-date certification revocation list (CRL) used to verify the validity of the CA's and user's / server's certificates if an on-line certificate validation mechanism via Online Certificate Status Protocol (OCSP) or Server-based Certificate Validation Protocol (SCVP) is not available?	• When an online certificate validation protocol such as OCSP or SCVP is not supported. CRLs must be made available for servers to client's certificates or for the clients to server's certificate if certificates are used for digital signature or authentication.		
5.9	CRL renewal When a CRL is used for certification validation, are cached copies of CRLs updated regularly? If so, please describe the frequency (e.g. once per day). Is the frequency of update commensurate with the associated risk of the application.	• CRL (Certificate Revocation Lists) must be updated periodically.		
5.10	Key Recovery Compliance if the application is subject to supervisory or data retention requirements such as SBP - psd/2014/C3-Annex or section 7 of PS&EFT Act 2007 or any other key recovery requirements, is there a key recovery process to fulfill the regulatory requirements?	• To comply with NBP policy or other regulatory requirements, key recovery must be enforced, such as encrypted transactional messages or data can be decrypted and recorded for regulatory compliance, log all Cryptographic module failures		
5.11	Unique Key Does each cryptographic key have a unique application domain? For each party, there should be as many different keys as there are different cryptographic functionalities.	• Any particular key should be used for one particular purposes (e.g. signing, data encryption, Key encryption etc.) • Keys used for in production environment must not be used for development or testing.		
6.0	Error Handling & Audit Logging			

6.1	Auditing and Events Does the application have an auditing capability across application layers? Depending on the risk of the application, are audit logs and alerts of unauthorized access maintained?	The answer should be "Yes" since to comply with the NBP IT policy section 2.3.5.5 Logging is performed before executing the transaction. If logging was unsuccessful (e.g. disk full, insufficient permissions) the application fails safe, this is for when integrity and non-repudiation are a must. Following significant events should be available for review: • ID Management (Create, Delete, Modify, Suspend, Resume) • Successful / Unsuccessful user login attempt • Account Lock out • Account Lock/Unlock • Group Creation • Creation or modification of application roles/ profiles • Creation/modification/deletion of user rights • Password Forget • Password Resets • Password Change • Change in Application/System security configuration • Alarms associated with a firewall or IDS/IPS • Financial Transaction or Sensitive PII data • Security Validation failure • Session Management failure • Application/Service Start/Stop • Suspicious/Fraud and other criminal activities		
6.2	Audit Events contents Does the individual audit event contain the necessary attributes?	Each log entry needs to include sufficient information for the intended subsequent monitoring and analysis. The application logs must record "when, where, who and what" for each event. All auditable events must give enough information to trace the event to a particulars but not limited to the following: • Unique log identifier • The user ID or the process ID of the event • System, application, module or component • Data and Time of the event • Application address e.g. IP address or machine name and port number • Resource ID e.g. window, url, page, form, method • Service Protocol • Source Address e.g. user/service IP address • Device Identifier e.g. IMEI, MAC • User, object Identity • Type of the event • Log Level • Success or failure of an event • Starting and ending time of access to the application • Description		

6.3	Admin activities Does security Administration activities for this system are logged and traceable to User ID?	To achieve the non-repudiation all the generic IDs should be escrowed and only accessible in case of emergency, each user must have its own ID and guarantees that an action can be proven to have originated from specific person.		
6.4	Audit Log Protection Are audit logs in store and during transmission, protected from unauthorized deletion, modification and disclosure? i.e. Administrator should not have the ability to modify / edit the logs	Audit Logs must be protected against unauthorized access to ensure its integrity and maintain accountability. The application does not output error messages or stack traces containing sensitive data that could assist an attacker, including Session ID and personal information.		
6.5	Audit Log File Configuration Can the audit log files be configured for log size and rollover to prevent log file data loss and a denial of service attack?	Audit Logs should be automatically roll over unless it can be ensured that the audit logs have been backed up or archived. Audit log file size should be configurable to prevent a denial of service attack or application handles log size issue automatically. Rollover must always be configurable.		
6.6	SIEM Integration Is application capable to integrate with SIEM	Application should be able to integrate with SIEM solution. SIEM is available which allows the analyst to search for log events based on combinations of search criteria across all fields in the log record format supported by this system.		
6.7	Audit Log Notification Are administrators warned when the audit logs are nearly full?	It is desirable to have a mechanism to warn administrator when the audit logs are nearly full to prevent an application from shutting down, from a denial of service or from overriding previous logs.		
6.8	Reports Does the application have an ability to generate custom audit reports based on the criteria specified by the log reviewer?	It is desirable to have a capability to generate audit reports based on a number of criteria specified by the log reviewer.		
7.0	Security Administration			
7.1	Functional ID If the application is using functional IDs (e.g. root in Linux/Unix, Administrator in Windows), are they protected against unauthorized usage?	It is important to list any functional Ids that exist and if any internal application or third party controls can be placed on the system to decrease the privileges associated with these accounts. Also controls should be in place for any system functional IDs to prevent unauthorized usage. In general, the existence of all power administration IDs is not desirable.		
7.2	Service Accounts Are service/database ids only used by the applications and not used by individual users or other processes	The application backend IDs such as database, service accounts are restricted and only allowed by the application. These accounts would not be accessible by any individual users.		
7.3	Separation of Roles Does the application split administration privileges into several accounts (e.g. system administration, Security Administration)?	According to the principle of least privilege it is desirable for administrative accounts to have the least privilege needed to perform a particular function. It is describable to have separate administrative roles to perform system management, security management and audit. If separation of roles cannot be enforced, then the		

		application must have provisions (e.g. auditing to ensure the accountability of the privileged accounts.		
7.4	Administrator's Conflict of Interest Does the application prevent a security administrator from performing transactions or administrative functions for themselves that conflict with this role?	The application should not allow security administrator to create or modify user accounts for themselves. In case there is a business requirement to allow such action, then an independent verification or maker/checker process must be implemented and all such actions must be audited.		
7.5	Maker/Checker for Administrative Actions Does the application support maker/checker or dual-control for administrative actions (e.g. account creation / modification, entitlement management).	It is describable to have internal maker/checker or dual-control for administration actions such as account creation/modification and entitlement management. When maker/checker or dual-control cannot be implemented, an independent verification process must be enforced.		
8.0	System Security and Availability			
8.1	Application Identity Is the application or web server running as a non-privileged user (e.g. non-root or non-administrator)?	If possible, the application or web server should run as non-privileged user, especially when this is a customer facing application. This provision should be implemented to reduce/control damage in case the application is compromised.		
8.2	Application Integrity Is there a mechanism to protect application configuration stores and maintain the integrity of critical application files?	It is important to protect application configuration stores and critical files with access control. This include all share folder for data and system files.		
8.3	BCP/DR Does the application support redundancy or replication for continuity of business or automatic fail-over?	Automatic fail-over is commonly required for mission-critical applications for high availability. However, some low criticality application may not have a BCP/DR requirement or manual process (last updated data restoration on contingency server). It is a business decision to determine whether it is required or not.		
8.4	DDOS attack Are controls in place to prevent a denial of service (DOS) attack on this system?			
9.0	Network Architecture and Perimeter Security			
9.1	Perimeter Security For Applications deployed in the DMZ, does the application prevent unauthenticated users from the Internet from accessing a server on our intranet?	For Internet applications, unauthenticated users must not be allowed to directly access the server or Intranet to prevent hackers from exploiting vulnerabilities on the server that would first compromise the server and then internal infrastructure. Users must be authenticated on a server in the DMZ (e.g. a web or VPN server) before interacting with another server on intranet. For B2B application, B2B server/devices must be placed in the DMZ to perform authentication.		

9.2	3-Tier Architecture Does the application support at least 3-Tier Architecture (e.g. web server, application server and backend server/database) to protect data from being directly accessed from the web server in the DMZ.	For Internal web applications, especially financial application or application that provide personal data, it is desirable to have at least a 3-tier architecture (3 tiers may include the tiers of web server, application server and backend server or database server)to protect the backend server/database from being directly accessed from the web server and being compromised.		
9.3	Persistent Storage on the DMZ if this is an Internet-based application, does the application prevent Confidential and above data from being persistently stored on a system in the DMZ?	Confidential and above category data should not be persistently stored on a system in the DMZ. i.e. Persistently stored means storage beyond the session lifetime.		
9.4	System-to-System Authentication Does the application support system-to-system authentication or the authentication at the application layer for communication between any two servers to prevent unauthorized access?	System-to-system authentication or authentication at the application layer should be implemented for communication between any two servers to prevent unauthorized access. Network access control such as SSL or IPsec could be used as a compensating control if system-to-system authentication or authentication at the application layer is not implemented. Note that IPsec is consider as the last resort.		
10.0	Session Management			
10.1	Session Management Does the authentication server(s) implements a session management mechanism to manage active login sessions and to prevent spoofing/masquerading?	Session management for this case is used to record the states of active login sessions and to retire inactive sessions when they time out. Session management should have the following properties: • Unique session identification • Session Identification that are protected in transit and in storage against unauthorized access. • An inactivity time out mechanism		
10.2	Application Logout Does the application have a logout functionality on every screen that is available for authenticated user?	When a user logs out, the application must completely log the user out and prevent the user from accessing pages or information that is available to active authenticated users.		
10.3	Session Identifier Generation Does the application generate session identifiers (IDs) with a sound pseudo-random number generator?	Session management is required for web applications because they are based on the stateless HTTP protocol. Therefore, session management is critical to the overall security of web applications. A sound session management scheme should be able to generate unique and unpredictable session IDs, restrict session lifetime, and protect session IDs.		
10.4	Session State Store Does the application protect its session state store against unauthorized access?	The session state store can be local or remote. Session state data should be protected against eavesdropping and unauthorized access. If session state store is remote then the data in transit should be encrypted with a secure protocol such as SSL or IPsec and the data in		

		store should be protected against unauthorized access.		
10.5	Session Lifetime Does the application restrict session lifetime and enforce the maximum login period for a session?	Prolonged session lifetime would increase the risk of session hijacking and reply attacks. Therefore the application should restrict session lifetime to reduce the risk. IS Policy requirements of inactive user session • 5 minutes for Critical System that are classified as sensitive; • 10-15 minutes for other classified systems based on business need		
10.6	Session Identification Passage Does the application prevent session identifiers from being passed over unencrypted channels?	If session IDs are used to track session states, then session IDs or cookies containing session IDs should be passed via encrypted channels (e.g. SSL/TLS) to prevent eavesdropping.		
10.7	Session Identifier Manipulation Does the application prevent users from manipulating session identifiers that are being passed in query string or from fields?	Session IDs should not be passed via query string or from fields because they can be easily modified by the users in an attempt to impersonate other users.		
10.8	Session Cookies Does the application encrypt session cookies?	Session (authentication) cookies should be encrypted to prevent session cookies from being stolen. Session cookie encryption along with SSL/TLS can mitigate the risk of cross-site scripting (XSS) attacks. Session cookies values that are created in insecure session should not be inherited in secure session cookies.		
10.9	Session Cookies Validation If session cookies are used by application, does the application validate the cookies before granting access to protected pages?	Cookies that contain Restricted or authentication data must be marked secure, so that they are sent only over encrypted channel, namely SSL/TLS. Cookies that contain Sensitive PII must be marked secured when transmitting via non-NBP manage infrastructures.		
10.10	Secure Cookies If the application uses cookies containing Sensitive or Higher information, are the cookies marked secured so that the cookies are sent only over encrypted channels AND is the cookies content encrypted using approved method?	Cookies that contain Sensitive+ data must be marked secure, so that they are sent only over encrypted channels, namely SSL/TLS. Cookies that contain Sensitive PII must be marked secured when transmitting via non-NBP managed infrastructures.		
11.0	Database Access			

11.1	Database Authentication Does the application server utilize the database authentication to directly connect to the database instead of user account authentication at the application level?	The Application Server may use a database account or an application account to establish the database connectivity. When the user accounts in the Application are tightly coupled with the database accounts, the database is accessible by all legitimate users on the platform. To enforce the principle of least privilege, it is more secure for application to use separate database accounts for DB authentication. In case where a user account on the Application server used to access the database, a least privileged account should be created.		
11.2	Database Password Protection in Storage Does the application protect/encrypt database connection strings (e.g. passwords) in local storage?	Database connection string contain authentication data and therefore must be encrypted in storage. Encrypted connection string and encryption keys must be protected. The function of decrypting connection string should be a standalone utility to prevent the connection string from being decrypted and display in the clear. Instead, it should be embedded into or fully integrated within the application.		
11.3	Database Password Protection in Transit Does the application enable/implement a secure protocol (e.g. SSL/TLS) to protect database passwords in transit?	If database connection string contains passwords it must be encrypted in the transit. In general, most database system support a secure protocol (e.g. SSL / TLS) for this purpose. When a secure protocol cannot be enabled or applied. IPsec or other secure protocol can be considered as a last resort for host-to-host encryption.		
12.0	Legal / Regulatory Compliance, Management Approval & Awareness			
12.1	Additional Legal or Regulatory Requirements Does the application comply with all regulatory / local laws which are not included in the Information Security policy.	Each and every application must comply with Legal/Regulatory/IS requirements.		
12.2	Banner Text Approval Is the Legal Department approved banner text, when supported by the application, displayed at all entry points where a user initially signs on?	If there is a need to support banner tax, legal-approved banner text must be displayed at all entry points where a user initially signs on either from local or remote access.		
13.0	Application Configuration and IS Processes			

13.1	Information Classification Has the information been classified in accordance with NBP Information Standards?	NBP TBML system(s) assets must be given a classification level in accordance with the NBP approved classification standard. • Confidential Information that is considered to be very sensitive to business and is intended for internal use only by following the need to know principle. Unauthorized disclosure of this level of information could seriously and negatively impact bank's reputation and may cause significant business loss. • Sensitive Information that requires a higher level of protection than normal from unauthorized disclosure or alteration. Unauthorized disclosure / alteration of such information may negatively impact bank's reputation or can cause legal implications. • Private Proprietary information that is being developed for NBP internal use and being shared among the NBP employees only. Property of NBP and disclosure of such information could affect the NBP business or employees. • Public Information either collected from public sources or being produced for public review. Disclosure of such information will not have an impact to NBP business & employees.		
13.2	Inherent Risk of the Application Has an inherent risk analysis been completed by the business during the definition phase of the project?	IS Risk Assessment is a mandatory requirement, Risk Assessment lifecycle must be completed in coordination of IS Risk team.		
13.3	Vendor Support Product Is the application software supported by an approved vendor?	Application vendor must be in the NBP's approved vendor list.		
13.4	Default Access Capability Are all default access capabilities (including passwords) removed, disabled or protected to prevent their unauthorized use?	No default ID should be used or enabled. Default IDs should be renamed and password split and escrowed with IS		
13.5	Vulnerability Assessment If required, has the application undergone all of the Application vulnerability Assessment and remediated all security findings as specified in the VA process.	If VA is required for this application, the required VA (Internal or External) must be performed and all security findings with the medium and High risk level must be remediated with the timeframe specified in the VA process.		
13.6	Masking Data Is sensitive PII information masked within the application whenever possible (displaying as well as printing)?	By the GLBA act, financial institutions must protect the security and confidentiality of customer's nonpublic personal Information (NPI). When NPI is being displayed or printed, it should be partially masked and only the last four digits can be displayed or printed for identification or verification.		

13.7	Configuration location are application configuration files protected from unauthorized access?	All security-relevant configuration information is stored in locations that are protected from unauthorized access.		
13.8	Configuration Error is application capable of handling configuration errors?	If the application cannot access its security configuration, all access to the application should be denied and do not allow access using default configuration.		
13.9	Audit Configuration Changes is auditing enabled to track application configuration changes?	All changes to the security configuration settings managed by the application are logged in the security event log.		
13.10	Fax Are automated or manual fax processes used in connection with the transection of data to/from the system? If yes describe the controls around the fax process.	If sensitive or above information must be sent over Fax, specific procedures and guidance must be created and followed to mitigate the risk. Fax cannot support user authentication nor data confidentiality. Manual authentication of the source and verification of the data may to be conducted to mitigate the risk and such action may need to be logged/recorded for accountability.		
14.0	Compliance			
14.1	3rd Party Solution is it certified by PCI, Common Criteria?	The solution related to Card processing must be certified by PCI, Common Criteria min Level 3+.		
14.2	Have any non-compliance being found as a result of this review? If True, provide corrective action plan and/or RA numbers in the "Open Issues and Approvals" TAB of this document			

Web Secure Coding Checklist (Bidder to provide response) *Bidder should complete this checklist in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.*		*Availability Response*	*Bidder Response*
1.0 Application Verification			
1.1	The integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes.		
2.0 Authentication			
2.1	All pages and resources require authentication except those specifically intended to be public.		
2.2	All password fields do not display the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.		
2.3	If a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.		
2.4	All connections to external systems that involve sensitive information or functions are authenticated.		

2.5	The forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.		
2.6	The username enumeration is not possible via login, password reset, or forgot account functionality.		
2.7	All authentication controls are enforced on the server side.		
3.0 Session Management			
3.1	The framework's default session management control implementation is used by the application.		
3.2	Sessions are invalidated when the user logs out.		
3.3	Sessions timeout after a specified period of inactivity.		
3.4	Sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		
3.5	All pages that require authentication to access them have logout links.		
3.6	The session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.		
3.7	The session id is changed on each login.		
3.8	The session id is changed on re-authentication.		
3.9	The session id is changed or cleared on logout.		
3.10	Only session ids generated by the application framework are recognized as valid by the application.		
3.11	Authenticated session tokens are sufficiently long and random to withstand attacks that are typical of the threats in the deployed environment.		
3.12	Cookies which contain authenticated session tokens/ids have their domain and path set to an appropriately restrictive value for that site. The domain cookie attribute restriction should not be set unless for a business requirement, such as single sign on.		
3.13	Verify that authenticated session tokens using cookies sent via HTTP, are protected by the use of "HttpOnly".		
3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and a strict transport security headers are present.		
3.15	Verify that the application does not permit duplicate concurrent user sessions, originating from different machines.		
4.0 Access Control			
4.1	Users can only access URLs for which they possess specific authorization.		
4.2	Direct object references are protected, such that only authorized objects are accessible to each user.		
4.3	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
4.4	Directory browsing is disabled unless deliberately desired.		
4.5	The same access control rules implied by the presentation layer which are enforced on the server side, such that controls and parameters cannot be re-enabled or re-added from higher privilege users.		

4.6	All user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.		
4.7	Verify the system can protect against aggregate or continuous access of secured functions, resources, or data. For example, possibly by the use of a resource governor to limit the number of edits per hour or to prevent the entire database from being scraped by an individual user.		
4.8	There is a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.		
4.9	Verify that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
4.10	Limitations on input and access imposed by the business on the application (such as daily transaction limits or sequencing of tasks) cannot be bypassed.		
4.11	All access controls are enforced on the server side.		
5.0 Input Validation			
5.1	The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.		
5.2	All input validation failures result in input rejection.		
5.3	All input validation or encoding routines are performed and enforced on the server side.		
5.4	Single/Centralized input validation control is used by the application for each type of data that is accepted.		
5.5	All input validation failures are logged.		
5.6	All input data is canonicalized for all downstream decoders or interpreters prior to validation.		
5.7	The runtime environment is not susceptible to SQL,LDAP,OS,XML Injection, or that security controls to prevent the Injection attacks.		
5.8	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
5.9	If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, verify that security sensitive fields such as accountBalance,role, password etc. are protected from malicious automatic binding.		
5.10	The application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)		
6.0 Output Encoding/Escaping			
6.1	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
6.2	All output encoding/escaping controls are implemented on the server side.		
6.3	Output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.		

6.4	All untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.		
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or are escaped properly.		
6.6	All untrusted data that are output to any interpreters not specifically listed above are escaped properly.		
6.7	For each type of output encoding/escaping performed by the application, there is a single/centralized security control for that type of output for the intended destination.		
7.0 Cryptography Requirements			
7.1	All cryptographic functions used to protect secrets from the application user are implemented on server side.		
7.2	All cryptographic modules fail securely.		
7.3	Access to any master secret(s) is protected from unauthorized access (a master secret is an application credential stored on disk which is used to protect access to security configuration information).		
7.4	Password hashes are salted uniquely when they are created.		
7.5	Cryptographic module failures are logged.		
8.0 Error Handling and Logging			
8.1	All logging controls are implemented on the server.		
8.2	Verify security logging controls, provide the ability to log both success and failure events that are identified as security-relevant.		
8.3	All events that include untrusted data will not execute as code in the intended log viewing software.		
8.4	Single logging implementation is used by the application.		
8.5	Application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.		
8.6	All code implementing or using error handling and logging controls is not affected by any malicious code.		
9.0 Data Protection			
9.1	All forms containing sensitive information have disabled client side caching, including autocomplete features.		
9.2	All sensitive data is sent to the server in the HTTP message body (i.e., URL/GET parameters are never used to send sensitive data).		
9.3	All cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		
9.4	There is a method to remove each type of sensitive data from the application at the end of its required retention period.		
10.0 Network Communication Security			
10.1	A path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each certificate is valid.		
10.2	Failed SSL/TLS connections do not fall back to an insecure connection.		

10.3	SSL/TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		
10.4	SSL/TLS connection failures are logged.		
10.5	Certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.		
10.6	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
10.7	There is a single standard SSL/TLS implementation that is used by the application that is configured to operate in an approved mode of operation		
11.0 HTTP Security			
11.1	"Redirect" (i.e. 302 Object moved) do not include unvalidated data. Form data redirect may be hijacked if compromised or mismanaged. If it is redirected to a site in a different domain, the users cannot tell whether the site is trusted or not before sensitive data contained in the form are submitted. Therefore, we recommend to NOT implement "redirect" when accepting sensitive information from user forms.		
11.2	The application accepts only a defined set of HTTP request methods, such as GET and POST.		
11.3	Every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).		
11.4	The HTTPOnly flag is used on all cookies that do not specifically require access from JavaScript.		
11.5	The secure flag is used on all cookies that contain sensitive data, including the session cookie.		
11.6	HTTP headers in both requests and responses contain only printable ASCII characters and do not expose detailed version information of system components.		
11.7	The HTTP header, X-Frame-Options is in use for sites where content should not be viewed in a 3rd-party X-Frame. A common middle ground is to send SAME ORIGIN, meaning only websites of the same origin may frame it.		
11.8	The application generates a strong random token as part of all links and forms associated with transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
11.9	The HTTP header can be easily manipulated by an attacker and must not be used for security decisions.		

Web Secure Coding Checklist (Bidder to provide response) *Bidder should complete this checklist in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.*		*Availability Response*	*Bidder Response*
1.0 Application Verification			
1.1	The integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes.		
2.0 Authentication			
2.1	All pages and resources require authentication except those specifically intended to be public.		
2.2	All password fields do not display the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.		
2.3	If a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.		
2.4	All connections to external systems that involve sensitive information or functions are authenticated.		
2.5	The forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.		
2.6	The username enumeration is not possible via login, password reset, or forgot account functionality.		
2.7	All authentication controls are enforced on the server side.		
3.0 Session Management			
3.1	The framework's default session management control implementation is used by the application.		
3.2	Sessions are invalidated when the user logs out.		
3.3	Sessions timeout after a specified period of inactivity.		
3.4	Sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		
3.5	All pages that require authentication to access them have logout links.		
3.6	The session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.		
3.7	The session id is changed on each login.		
3.8	The session id is changed on re-authentication.		
3.9	The session id is changed or cleared on logout.		
3.10	Only session ids generated by the application framework are recognized as valid by the application.		
3.11	Authenticated session tokens are sufficiently long and random to withstand attacks that are typical of the threats in the deployed environment.		
3.12	Cookies which contain authenticated session tokens/ids have their domain and path set to an appropriately restrictive value for that site. The domain cookie attribute restriction should not be set unless for a business requirement, such as single sign on.		

3.13	Verify that authenticated session tokens using cookies sent via HTTP, are protected by the use of "HttpOnly".		
3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and a strict transport security headers are present.		
3.15	Verify that the application does not permit duplicate concurrent user sessions, originating from different machines.		
4.0 Access Control			
4.1	Users can only access URLs for which they possess specific authorization.		
4.2	Direct object references are protected, such that only authorized objects are accessible to each user.		
4.3	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
4.4	Directory browsing is disabled unless deliberately desired.		
4.5	The same access control rules implied by the presentation layer which are enforced on the server side, such that controls and parameters cannot be re-enabled or re-added from higher privilege users.		
4.6	All user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.		
4.7	Verify the system can protect against aggregate or continuous access of secured functions, resources, or data. For example, possibly by the use of a resource governor to limit the number of edits per hour or to prevent the entire database from being scraped by an individual user.		
4.8	There is a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.		
4.9	Verify that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
4.10	Limitations on input and access imposed by the business on the application (such as daily transaction limits or sequencing of tasks) cannot be bypassed.		
4.11	All access controls are enforced on the server side.		
5.0 Input Validation			
5.1	The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.		
5.2	All input validation failures result in input rejection.		
5.3	All input validation or encoding routines are performed and enforced on the server side.		
5.4	Single/Centralized input validation control is used by the application for each type of data that is accepted.		
5.5	All input validation failures are logged.		
5.6	All input data is canonicalized for all downstream decoders or interpreters prior to validation.		

5.7	The runtime environment is not susceptible to SQL,LDAP,OS,XML Injection, or that security controls to prevent the Injection attacks.		
5.8	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
5.9	If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, verify that security sensitive fields such as accountBalance,role, password etc. are protected from malicious automatic binding.		
5.10	The application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)		
6.0 Output Encoding/Escaping			
6.1	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
6.2	All output encoding/escaping controls are implemented on the server side.		
6.3	Output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.		
6.4	All untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.		
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or are escaped properly.		
6.6	All untrusted data that are output to any interpreters not specifically listed above are escaped properly.		
6.7	For each type of output encoding/escaping performed by the application, there is a single/centralized security control for that type of output for the intended destination.		
7.0 Cryptography Requirements			
7.1	All cryptographic functions used to protect secrets from the application user are implemented on server side.		
7.2	All cryptographic modules fail securely.		
7.3	Access to any master secret(s) is protected from unauthorized access (a master secret is an application credential stored on disk which is used to protect access to security configuration information).		
7.4	Password hashes are salted uniquely when they are created.		
7.5	Cryptographic module failures are logged.		
8.0 Error Handling and Logging			
8.1	All logging controls are implemented on the server.		
8.2	Verify security logging controls, provide the ability to log both success and failure events that are identified as security-relevant.		
8.3	All events that include untrusted data will not execute as code in the intended log viewing software.		
8.4	Single logging implementation is used by the application.		

8.5	Application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.		
8.6	All code implementing or using error handling and logging controls is not affected by any malicious code.		
9.0 Data Protection			
9.1	All forms containing sensitive information have disabled client side caching, including autocomplete features.		
9.2	All sensitive data is sent to the server in the HTTP message body (i.e., URL/GET parameters are never used to send sensitive data).		
9.3	All cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		
9.4	There is a method to remove each type of sensitive data from the application at the end of its required retention period.		
10.0 Network Communication Security			
10.1	A path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each certificate is valid.		
10.2	Failed SSL/TLS connections do not fall back to an insecure connection.		
10.3	SSL/TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		
10.4	SSL/TLS connection failures are logged.		
10.5	Certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.		
10.6	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
10.7	There is a single standard SSL/TLS implementation that is used by the application that is configured to operate in an approved mode of operation		
11.0 HTTP Security			
11.1	"Redirect" (i.e. 302 Object moved) do not include unvalidated data. Form data redirect may be hijacked if compromised or mismanaged. If it is redirected to a site in a different domain, the users cannot tell whether the site is trusted or not before sensitive data contained in the form are submitted. Therefore, we recommend to NOT implement "redirect" when accepting sensitive information from user forms.		
11.2	The application accepts only a defined set of HTTP request methods, such as GET and POST.		
11.3	Every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).		
11.4	The HTTPOnly flag is used on all cookies that do not specifically require access from JavaScript.		
11.5	The secure flag is used on all cookies that contain sensitive data, including the session cookie.		

11.6	HTTP headers in both requests and responses contain only printable ASCII characters and do not expose detailed version information of system components.		
11.7	The HTTP header, X-Frame-Options is in use for sites where content should not be viewed in a 3rd-party X-Frame. A common middle ground is to send SAME ORIGIN, meaning only websites of the same origin may frame it.		
11.8	The application generates a strong random token as part of all links and forms associated with transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
11.9	The HTTP header can be easily manipulated by an attacker and must not be used for security decisions.		

API Security Review Checklist (Bidder to provide responses, If applicable)			Availability Response	Bidder Response
INSTRUCTIONS: Fill in all applicable sections.		Guide		
1.0	Authentication & Authorization	Acceptable Criteria	(Yes/No)	
1.1	Use secure authentication mechanism	Don't use basic authentication with plaintext credentials e.g. plaintext password in URL parameter etc. Apply standard & secure authentication such as JWT tokens with dynamic mechanism per session/per request, OAuth 2.0, or public/private API keys combination.		
1.2	Ensure secure storage of passwords, API tokens & keys	Store API tokens/keys in secure key vaults via secure mechanism such as Windows Local Security Authrority so that tokens & keys remain secure including the config file data.		
1.3	Ensure encryption of sensitive data & tokens in transit and at rest	Sensitive data including credentials must be encrypted in transit and at rest. Use transport layer security protocols and strong encryption algorithms e.g. RSA, AES-256 etc.		
1.4	Never place the credentials in source code	Plaintext credentials or hashes must not be placed in source code to avoid misuse & brute force attacks by adversaries.		
1.5	Configure maximum login retries following the IS policy of organization	For NBP assets, 5 maximum retries should be allowed before the account gets locked. It prevents brute force attacks.		
2.0	Access Security			
2.1	Use HTTPS insead of HTTP	Implement SSL based communication over API connections.		
2.2	Display as minimum information as possible in you API request/response	Don't rely on client side to filter data; Avoid using generic methods such as to_json() and to_string(). Instead, cherry-pick specific properties & data you really want to return.		
3.0	Input Security			

3.1	Sensitive data protection in URL	Don't use any sensitive data (credentials, passwords, security tokens, and/or API keys) in the URL but use standard Authorization header.		
3.2	Use appropriate HTTP method according to the operation	Use GET (read), POST (create), PUT/PATCH (replace/update), and DELETE (to delete a record) methods appropriately in API communication. Respond with *405 Method Not Allowed* if the requested method is not appropriate for the requested resource.		
3.3	Ensure content validation controls for input security	Content Validation for Request: To validate the content type of response, use Accept header in HTTP request (Content Negotiation) to allow only the supported formats (e.g., application/xml, application/x-www-form-urlencoded, multipart/form-data, application/json etc.). Content Validation for SQL injection, RCE and XSS: Validate the user-submitted content for SQL injection, Remote Code Execution, and Cross-Site Scripting (XSS).		
3.4	Ensure Secure Coding Practice	Remove unused dependencies, unnecessary features, components, files, and documentation. Run depenciy check tools such as OWASP Dependency check.		
3.5	Make trusted updates of packages	Always check for trusted sources. Get the packages for your application with authorized signature so that no malicious component is included in the package.		
3.6	Apply caching and rate limiting	Use an API Gateway service to enable caching, rate limit policies (e.g., Quota, Spike Arrest, or Concurrent Rate Limit) and deploy API resources dynamically.		
4.0	Output Security			
4.1	Ensure content validation controls for output security	Content Validation for Response: Validate the content type of returned data via Content-type header of HTTP response. It should match with the request's Accept header. Respond with 406 Not Acceptable response if it is not matched.		
4.2	Use appropriate HTTP response headers for output security	Recommended Use: • X-Content-Type-Options: Nosniff • X-Frame-Options: Deny (if there are no frames used in application) • X-Frame-Options: Sameorigin (in case frames are to be used in application) • Content-Security-Policy: default-src 'none' • Remove fingerprinting headers like *X-Powered-By*, *X-AspNet-Version*, etc. • Don't return sensitive data like credentials or security tokens in response • Return the proper status code according to the operation completed (e.g., 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).		
5	Data Processing Security			

5.1	Ensure Object level authorization	• User's own resource ID should be avoided. Use /me/orders instead of /user/654321/orders • Don't auto-increment IDs. Use UUID instead		
5.2	Ensure XML External Entities (XXE) prevention	• Enternal entites' misconfiguration may lead to SSRF (Server-Side Request Forgery) and billion laugh attacks. Configure the XML parser to disable external entity resolution • The XML parser should be configured to use a local static DTD and disallow any declared DTD included in the XML document		
5.3	Ensure data rate limiting	.Rate limit the data processing wherever applicable in order to avoid brute force attacks.		
5.4	Do not use test environment in production mode	Make sure your application is set to production mode before deployment. Running a debug API in production could result in performance issues & unintended operations such as test endpoints and backdoors. It may expose data sensitive to the organization or development team.		
6	Monitoring Security			
6.0	Ensure API logging & monitoring mechanism	The API logs must be stored in a centralized log management system. API monitoring includes auditing, logging, and version control for all APIs and their components. This helps in the troubleshooting process when and if a problem occurs.		
6.1	Limit number of API calls	Set a quota on the API calls count, i.e. put limitations on the number of times an API is called.		

Annexure-II: Cloud Based Checklist

Cloud Based Outsourcing Service Arrangements Cloud Service Provider's (CSP) Compliance Matrix				
Clause ID	Clause Description			
		Consent/comments by Responsible functions	Existing Controls at CSP	Remarks (If Any)
E. PERMISSIBLE CLOUD OUTSOURCING ARRANGEMENTS				
1	Please confirm whether this service/function is material or non-material as per below mentioned definition provided by SBP. 1. For the purpose of these regulations, material workload means all systems, applications, and services that are fundamental for carrying out business of an RE (Regulated Entity)/bank, and if disrupted, have the potential to significantly impact an institution's business operations, reputation or profitability.			

	2. REs may outsource their workloads to CSPs in the following manner: a) All type of workloads (i.e. material and non-material) may be outsourced to reputable onshore (i.e. domestic) CSPs; b) EMIs, non-designated PSOs/ PSPs may outsource their material and non-material workloads to offshore (i.e. outside Pakistan) CSPs; c) Banks, MFBs, DBs, DFIs and designated PSOs/PSPs may outsource their non-material workloads to offshore CSPs. However, outsourcing of their material workloads to offshore CSPs shall be subject to SBP approval whereby SBP may grant approval on case to case basis, after considering the following: i. Systemic implications of the CO (cloud outsourcing) arrangement ii. Institution specific risks iii. Legal and other strategic risks iv. Data processing and storage v. Availability and quality of services vi. Security and other controls vii. Contingency and exit planning viii. Resilience ix. Sub-contracting x. Assurance mechanism xi. Role and responsibilities d) For approval to outsource material workloads to offshore CSPs, banks, MFBs, DBs and DFIs shall submit their request to BPRD whereas designated PSOs/PSPs shall submit it to PSP&OD; e) While granting approval to banks, MFBs, DBs, DFIs and designated PSOs/PSPs, SBP may impose additional terms and conditions over and above the requirements of this framework; f) For CO arrangements, REs may use any service and deployment model as per their requirements and risk appetite; g) REs shall give preference to onshore CSPs for outsourcing their workloads; h) REs shall not process and store their data in unfriendly or hostile jurisdictions;			
	3. Outsourcing of services to CSPs does not absolve the REs from their prime responsibilities including managing and running the business operations effectively, legal and regulatory compliance, and protection of customers' data.			
	4. SBP may instruct any RE to restrict outsourcing of their workloads to CSPs due to its systemic impact, unacceptable risks and any other concerns.			
	5. REs shall submit details of their CO arrangements to SBP, as and when required.			

	6. SBP may instruct REs to shift their cloud based workloads to SBP designated onshore community cloud as and when the same is available.			
F. GOVERNANCE				
2	1. Develop a comprehensive policy for CO duly approved by their BoD. In this regard, the REs can also amend their existing 'Policy for Outsourcing Arrangements' to include/update CO. The policy shall encompass all services, as per requirements provided in section E above that can be outsourced to CSP, and at least include all those aspects that have been prescribed in this framework.			
	2. Conduct appropriate due diligence of CSPs and proactively identify any risks emanating from their CO arrangements including risks associated with sub-contracting by CSPs.			
	3. Update their Enterprise Risk Management framework or other relevant policies for effective oversight and management of risks emanating from the CO arrangement(s). The framework shall include sub-contracting risks, assessment of cloud service location(s) especially if outside Pakistan with specific focus on areas including but not limited to legal aspects; regulatory issues; jurisdictional concerns; availability; security and resilience of information assets and services; connectivity; political and security situation; ease of oversight; plausibility of RE, SBP and external audit staff to travel for onsite assessment/ audit or alternate assurance mechanism.			
	4. Delegate cloud specific governance responsibilities such as for overseeing adherence to regulatory as well as performance requirements, including cloud service SLAs, reviewing of KPIs and KRIs, incidents (including cybersecurity incidents) and other relevant matters to the ITSC. In this regard, the ToRs of ITSC shall be suitably amended to include these responsibilities			
	5. Undertake all CO arrangements through legally binding SLAs, which shall at least include the areas prescribed in Appendix – I. These SLAs must be vetted by the legal function of the RE and be executed by the REs (except branches of foreign banks) themselves instead of their parent company or subsidiary, with governing law preferably as law of Pakistan. However, compliance with the laws of Pakistan, along with compliance to any legal obligation as prescribed by the host country of the CSP, shall be mandatory at all times.			
	6. Define and agree upon the roles and responsibilities of the IT and operational departments (e.g. requirement analysis, performance testing, UAT, responsibility for data validation, etc.), before transferring information assets and services to a CSP.			

	7. Ensure that the CO arrangements are compliant with the relevant legal and regulatory requirements, and the IA functions of the REs shall provide independent certification to their BoDs in this regard.			
G. DUE DILIGENCE OF CLOUD SERVICE PROVIDER				
3	REs shall exercise reasonable care before entering into CO arrangements. To ensure effective management of the associated risks, REs shall conduct reasonable due diligence of the CSPs and their material sub-contracting arrangements by using defined criteria which shall include the following:			
	1. Evaluation of feasibility of CO arrangements including cost effectiveness, quality of service, and legal / regulatory / compliance risks.			
	2. Ability of CSP to meet legal and regulatory requirements of Pakistan.			
	3. Assessment of financial strength and resources.			
	4. Competence, business structure, experience, track record in delivering such services.			
	5. Assessment of CSPs ability to comply with necessary minimum controls including physical security / internal controls based on the intended workloads, especially with respect to confidentiality, integrity, availability and resilience.			
	6. Assessment of corporate governance and entity level controls.			
	7. Assessment of CSPs ability to provide REs the control over data residency enabling them to shift over preferred data center instance, depending upon the cloud service model, in order to host these services at such locations/countries/regions considering geopolitical risks.			
	8. Cybersecurity and IT capabilities including adherence to international standards and best practices.			
	9. Sub-contracting risk management.			
	10. Data security related controls.			

	11. Access, audit and information rights of REs, SBP and external auditors of the REs.			
	12. Support services.			
	13. Contingency, resilience and exit arrangements.			
	14. Up to date certification and attestation of the CSPs including but not limited to IT service delivery, business continuity & disaster recovery, cyber / information security, and data center Tier III certification.			
	15. Liability of claims / penalties on CSPs for: a) Unauthorized transactions; b) Service disruptions; c) Security breaches; d) Enforcement and penal actions that may be taken by regulatory and legal authorities against the REs for not complying the regulatory and legal requirements, due to faults by CSPs.			
	16. For material workloads: a) Threat & Vulnerability Assessment or equivalent independent assessments of data centers to identify the security and operational weaknesses. The scope of such assessments shall include physical and environmental security, perimeter security, access controls, security & emergency procedures, monitoring, redundancy, natural disasters, and the political and economic climate of the country in which the data center resides. The assessment shall cover all data centers where the REs' data / systems will reside; b) Independent assessments instead of solely relying on attestations by the CSPs, and the results shall be reviewed by REs' IA as well as Information Security (IS) function. However, the REs may consider SOC Reports (level 1, 2 & 3).			
H. OVERSIGHT				
4	The risk exposures and effectiveness of the corresponding controls may vary over the tenure of the CO arrangements. In this regard, REs shall:			
	1. Develop and maintain an effective oversight mechanism including but not limited to the assessment of performance against desired service levels and ongoing viability of the CSP and its services, cybersecurity practices and controls, changes in service location(s), sub- contracting, change of ownership, control environment; and timely response to emerging risks and issues.			
	2. On an ongoing basis, review and monitor the CSP's compliance with legal, regulatory and contractual obligations.			

	3. Monitor access to their cloud data/workloads, wherever possible such as through cloud activity reports.			
	4. Review internal control assessment / audit reports of the CSPs, in order to obtain assurance regarding the security and resilience.			
	5. For material workload, conduct comprehensive audit of the CSPs, either themselves or through third party assessors / pooled audits, at least once in two years. The scope of the audit shall at least include the infrastructure and related software used to deliver cloud services to the RE. However, in case where audit/onsite assessment cannot be conducted due to a valid reason(s), REs may rely on internationally recognized third party certifications and reports made available by the CSPs, after sufficient understanding and review of their scope, methodology and the ability of the assessors.			
I. CONTINGENCY PLANNING				
5	REs shall develop contingency plan for their CO workloads in order to deal with any disruption/degradation of cloud related services. The contingency plan shall take into account all possible scenarios regarding the unavailability of CSP related services due to various reasons such as technical/connectivity issues, inability of CSP to provide services due to legal actions in their respective jurisdictions, etc. In this regard, REs shall:			
	1. Prudently select appropriate implementation option (service and deployment model, availability zones, server/server-less, etc.) along with related communication technologies, to offer better resilience that commensurate with their workload.			
	2. Maximize the redundancy by design and workload distribution, and implement health and monitoring checks for ensuring HA of their cloud workloads.			
	3. Ensure redundant and robust connectivity arrangements through different international internet cables and include penalties for disruption and downtimes in their agreements.			
	4. Define clear roles and responsibilities including responsibility for signing off, updating and activating the contingency plan.			
	5. Periodically review and update the contingency plan, taking into account developments which may affect their feasibility. These may include increase in number of availability zones, changes in business requirements, new viable alternate CSPs, technological changes, etc.			

	6. Periodically (at least once annually) test the contingency plan against various scenarios including disruption of internet / communication services, unavailability of CSP, etc. Where possible, REs may conduct collaborative testing of their contingency plan with their CSPs. Further, the REs shall ensure that the deficiencies identified during testing are recorded and corrective actions are implemented.			
J. RIGHT TO AUDIT, ACCESS AND INFORMATION				
6	REs shall ensure that CO does not hinder SBP in conducting its supervisory functions. In this regard, the REs shall comply with the following requirements:			
	1. Ensure that their internal & external auditors/ independent assessors and SBP have right to conduct audits and onsite assessments of the CSP and its sub-contractors, if required. Further, there should be no restriction or prohibition on access to REs' cloud related information assets and services for the RE, its auditors, independent assessors or SBP's authorized staff or such visits are otherwise not impractical.			
	2. Ensure that access, audit and information rights provided through the contractual arrangement include where relevant: a) Premises, data, devices, information, systems, and networks used for providing the cloud services or monitoring its performance. These may include CSP's (and its sub-contractors) policies, processes, and controls; b) Results of security testing carried out by CSP or on its behalf, on its applications, data, and systems to assess the effectiveness of the implemented cybersecurity processes and controls; c) Results of security testing carried out by the sub-contractors or on its behalf, on its applications, data, and systems, where applicable, to ascertain effectiveness of the cybersecurity processes and controls; d) Company and financial information; e) CSPs' external auditors, personnel, and premises.			
	3. In case, where audit/onsite assessment cannot be conducted for a valid reason(s), REs may rely on internationally recognized third party certifications, and reports made available by the CSP. However, reliance on these third party certifications and reports shall be supported by adequate understanding and review of the scope, the methodology applied therein and the ability of the third party and CSP to clarify matters relating to the assessment. Further, the REs shall have contractual right to request for the expansion of the scope of the certifications / assessments / audits to cover relevant controls and systems.			

	4. Ensure that CSPs timely provide any information requested by SBP, whenever required.			
	5. Follow up with the CSP to ensure that all appropriate and timely remediation actions are taken to address any audit findings.			
K. EXIT PLANNING				
7	REs shall develop an exit plan by considering the materiality and impact of their workloads outsourced to CSPs. In this regard, REs shall comply with the following requirements:			
	1. Ensure that the exit plan covers scenarios for stressed and non-stressed exit circumstances.			
	2. Ensure that the exit plan has defined trigger events, alternative solutions, transition plans, and roles and responsibilities including responsibility for signing off, updating and activating the plan.			
	3. Periodically review and test the exit plan, taking into account developments which may affect its feasibility.			
	4. Implement measures including but not limited to contractual or escrow arrangements, to ensure continuity of critical business services in case of exit.			
	5. Ensure complete removal of data including logs from all locations of CSP in case of exit.			
	6. To avoid the lock-in and dependency risks, REs shall in their CO arrangement contracts: a) Avoid inclusion of any lock-in clause or exclusivity arrangements; b) Ensure that they have right to terminate the CO agreement at least in the following circumstances: i. Change in ownership of the CSP ii. Insolvency or liquidation of the CSP iii. CSP goes into judicial administration iv. CSP is in breach of applicable laws, regulations or contractual provisions v. Significant and material breach of security or confidentiality vi. Demonstrable deterioration to perform the contracted service c) Ensure that the minimum termination period is documented in their CO contracts.			
L. SUB-CONTRACTING				

8	The CO arrangements expose REs to various risks relating to sub-contracting due to improper/non implementation of controls by the sub-contractors. For material sub-contracting, the REs shall comply with the following requirements:			
	1. Have visibility of the CSP supply chain by ensuring that the CSP maintains and provides an updated list of its sub-contractors.			
	2. Consider potential impact of large, complex sub-contracting by the CSPs on their operational resilience, and ability to oversee and monitor the emanating risks.			
	3. Only permit sub-contracting by CSPs if such arrangements do not give rise to excessive operational risks, and sub-contractor agrees to comply with all applicable legal, regulatory, contractual, audit and access requirements including granting REs and SBP contractual access, audit and information rights.			
	4. Review material sub-contracting agreements of the CSP and ascertain that the legal, regulatory, operational, and cybersecurity requirements are complied with, throughout the supply chain.			
	5. Ensure that the CSPs have the capability and capacity to oversee any material sub- contracting on an ongoing basis.			
M. USER ACCESS MANAGEMENT AND AUTHENTICATION				
	REs shall implement complete life cycle of user access management for their cloud related workloads, while complying with the following requirements:			
	1. Implement at-least four eye principle for user access administration.			
	2. Periodically review user access right changes independently.			
	3. Ensure that the use and access of service, generic and administrative accounts are controlled and monitored. Moreover, the REs shall implement MFA and limit use of these accounts through dedicated machines only.			
	4. Create separate account of administrative users for routine operations, and implement enhanced password controls (length, complexity, age).			
	5. Implement MFA and IP source restrictions (wherever possible) for their users accessing cloud environment.			
	6. Monitor and document the use of master account, and permit its usage only under exceptional circumstances.			

	7. Implement access controls for data backups including log data, of cloud related workloads.			
	8. Ensure that CSPs do not have access to REs' systems, software and data.			
N. CHANGE AND CONFIGURATION MANAGEMENT				
	REs shall plan and implement configuration management in conjunction with IT change management to ensure safe and secure operations of cloud services. In this regard, REs shall comply with the following requirements for their cloud related workloads:			
	1. Implement mechanism for detecting unauthorized changes to cloud environment, and configure automated alerts for the changes.			
	2. Ensure CM procedures for cloud related workloads are documented and mutually agreed with the CSP. These shall at least include change request and approval procedures, change prioritization and impact assessment, change reporting, roles and responsibilities, timeframe for patching and software releases.			
	3. Ensure that the CSPs have well-defined and robust CM controls, and notify the REs in advance of the changes.			
	4. Ensure that the changes are tested before their implementation on the production environment.			
	5. Define roles and responsibilities of REs staff for configuration management of the cloud environment, and at least segregate infrastructure, security and application roles.			
	6. Create and maintain baselines for cloud hosted systems, and periodically review, monitor, report and remediate non-compliance with the baselines.			
O. INCIDENT MANAGEMENT				
9	Effective and efficient remediation of the incidents requires timely detection and proper integration with the incident response and management processes. With the increase in sophistication of cyber-attacks, there is a need to use advance analytics to correlate events across multiple systems. For incident management, REs shall comply with the following requirements for their cloud related workloads:			

	1. Define and document criteria, performance requirements and procedures for escalation, notification, containment and closure of incidents (including IT, cyber incidents) in consensus with the CSP(s).			
	2. Ensure access to incident and root cause analysis reports of the CSPs.			
	3. Designate a SIRT to provide timely response to IT/cyber incidents. In this regard, roles and responsibilities of CSP and REs' teams shall be formalized.			
	4. Ensure that CSPs shall provide reasonable access to necessary information to assist in any REs' investigation arising due to an incident in the cloud.			
	5. Ensure that the CSPs conduct formal post incident review of the material cloud related incidents and provide their report to the RE.			
	6. Ensure that ITSC as part of their oversight reviews and discusses cloud related incidents.			
	7. Periodically review and test Incident Response Plan of cloud related workloads at least once annually, keeping in view cybersecurity as one of key considerations.			
P. DATA SECURITY				
10	Outsourcing of the workloads to the CSPs does not relieve the REs from the responsibility of safeguarding data confidentiality and integrity. In this regard, REs shall:			
	1. Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms.			
	2. Desensitize the production data before porting or using it on non-production environment(s).			
	3. Ensure that their data in the cloud environment is clearly identifiable and segregated.			
	4. Take appropriate measures for the protection of Personally Identifiable Information (PII); and ensure compliance with the requirements of laws of Pakistan at all times. Further, REs shall ensure that CSPs do not disclose their data to any third party including foreign governments / courts / law enforcement agencies without their consent.			
	5. Ensure that CSP does not use their data for any commercial purposes.			

	6. Implement reasonable backup and restoration testing mechanism, depending on the nature of the workloads in compliance with the defined RPOs. Further, the backup mechanism shall have ransomware protection, and the backup restoration testing exercise shall be conducted at least on a half-yearly basis.			
	7. Classify information assets in terms of their sensitivity, confidentiality & availability, and implement additional controls for high value cloud information assets.			
	8. Implement controls to prevent unauthorized exfiltration of data from the cloud environment. These controls shall include deployment of content inspection technologies, controls on data downloading and extraction, monitoring unusual data access, etc.			
	9. Ensure that they are notified about any proposed change in the location of their data, and have contractual right to reject such change, or terminate the CO arrangement on such grounds.			
	10. Ensure that data is deleted from all storage locations of the CSP following an exit or termination of the CO arrangement, and where applicable, from the systems of any sub- contractor by requesting written confirmation from the CSP.			
Q. CRYPTOGRAPHIC KEY MANAGEMENT				
11	CSPs use cryptographic controls to secure access and segregate customers' data. Hence, the security of the cryptographic keys is critical for ensuring the data security. CSPs offer a variety of key management options/features, which can be selected by the REs for implementation based on the significance of their workloads. In this regard, the REs shall comply with the following requirements:			
	1. Develop and implement policies and procedures governing the lifecycle of the cryptographic material.			
	2. Ensure that details of the cryptographic algorithms and other related parameters such as key lengths, renewals etc. are reviewed by a subject matter expert.			
	3. Ensure that details of the location, ownership and management of the encryption keys and HSM are agreed with the CSP and documented.			
	4. Ensure that the cryptographic keys are unique and generated only by the REs. Further, REs must have the sole ability to administer/manage these keys and HSM.			
	5. Periodically change the cryptographic keys in accordance with the international standards and best practices			

	6. Ensure that the encryption keys are stored separate from the virtual images and information assets.			
	7. For material workloads, deploy/implement HSM with due controls.			
R. TOKENIZATION				
12	Depending on the sensitivity of data workload, REs may implement tokenization to minimize the data footprint. While implementing tokenization, REs shall assess and evaluate the features and data interactions of the tokenization solution. REs shall also ensure that the CSPs do not have access or control over the tokenization solution.			
S. NETWORK ARCHITECTURE				
	The network structure and logical layout is of paramount importance in any cloud implementation. Therefore, the REs must implement controls for protection against plausible threats/attacks including cloud specific attacks, by implementing the following requirements:			
	1. Ensure security of their CO arrangements and on premise environments by implementing controls at appropriate locations to detect and mitigate security breaches and ongoing attacks. These controls shall include but not limited to perimeter security, network IDS/IPS, WAF, DDoS protection, etc.			
	2. Implement network segmentation based on type of workloads (e.g. production, pre- production, quality assurance, development, etc.) and purpose (e.g. end-users, critical servers, other servers, middleware, interface, etc.). In this regard, a dedicated network segment (i.e. management network) not accessible from other operational segments shall be implemented for administration purposes. Further, all internet traffic shall be routed through a dedicated network segment (i.e. security segment) and other network segments shall not have direct internet access.			
	3. Secure traffic between the cloud and on premise environment using a VPN or direct network connection with stringent access control rules configured to ensure routing of traffic from/to dedicated source and destination IPs.			
	4. Monitor and control access to and security of the cloud environments. In this regard, regularly review the firewall rules and access lists, especially after any changes.			
T. SECURITY TESTING				

13	The dynamic and evolving nature of cyber threats requires a high degree of validation and testing of security posture of an enterprise, on periodic basis. However, security testing of the systems and applications in the cloud environment is challenging due to the inherent shared service model. In this regard, REs shall comply with the following requirements:			
	1. Conduct vulnerability assessment, penetration testing and scenario based security testing of their systems hosted with the CSPs on periodic basis, at least once annually.			
	2. Ensure that CSPs conduct vulnerability assessment and penetration testing for the infrastructure and applications managed by them, at least once annually in order to provide security assurance to the REs. Further, the REs shall be fully cognizant of the scope of such assessments while examining the results.			
	3. Ensure that security testing is conducted while taking into consideration various scenarios and threats that are unique to cloud services including but not limited to hypervisor jumping, weak application programming interfaces, DoS hyper jacking, wrapping attacks, cloud malware injection, side channel attacks, etc.			
	4. Ensure that all vulnerabilities identified for their cloud related workloads are categorized in terms of risk, tracked and rectified (including post validated). For the infrastructure and applications managed by the CSPs, REs shall implement alternate mechanism for obtaining assurance that the vulnerabilities are timely rectified.			
	5. In case of material CO, ensure independent Threat & Vulnerability Assessment of CSP's data centers hosting the data/systems of REs, at least once annually.			
U. SECURITY EVENT MONITORING				
14	REs shall establish mechanisms for SEM by complying with the following requirements:			
	1. Wherever possible, leverage the controls/tools available in the cloud environment to enforce consistent security standards and baselines, automated response, remediation and notification.			
	2. Integrate CSP related services with their SIEM solutions to provide a detailed analysis of the security logs. In this regard, cloud specific incident scenarios with correlation rules shall be implemented. Further, AI and ML driven technologies may be explored and preferably adopted, where available.			
	3. Ensure that cloud related activities are effectively monitored by their SOC on 24x7 basis.			
V. OTHER REQUIREMENTS				

15	1. REs shall monitor and review capacity utilization of their cloud workloads.			
	2. REs shall provide adequate training of the cloud environment, to their end-users and privileged users.			
	3. All security incidents / breaches shall be reported to SBP in compliance with the requirements specified in the 'Enterprise Technology Governance & Risk Management Framework for Financial Institutions' or as advised by SBP from time to time. Further, REs shall conduct investigations to identify the root cause, take appropriate actions to prevent recurrence of such incidents in future and fix responsibility for such lapse.			
	4. For material workloads, REs shall provide following information to SBP1 one month before placing their services with the CSPs: a) Name of the CSPs, and their parent company (if any); b) Description of the activities and details of data to be placed with the CSP; c) Date of commencement / renewal / expiry of services; d) Last contract renewal date (where applicable); e) Service and Deployment Models.			

SECTION VI: STANDARD FORMS

Form 1 (A) Letter of Bid For Technical Proposal

INSTRUCTIONS TO BIDDERS: (delete this box once you have completed the document)

*Place this Letter of Bid in the **first** envelope "**TECHNICAL PROPOSAL".***

The Bidder must prepare the Letter of Bid on stationery with its letterhead clearly showing the Bidder's complete name and business address.

Note: All italicized text in black font is to help Bidders in preparing this form and Bidders shall delete it from the final document.

Date of this Bid submission: [*insert date (as day, month and year) of Bid submission*]
RFB No.: [*insert number of bidding process*]
Request for Bid No.: [*insert identification*]

We, the undersigned Bidder, hereby submit our Bid, in two parts, namely:

(a) the Technical Proposal, and
(b) the Financial Proposal.

In submitting our Bid we make the following declarations:

(a) **No reservations:** We have examined and have no reservations to the bidding document, including addenda issued in accordance with Instructions to Bidders (ITB 9);
(b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITB 3;
(c) **Bid/Proposal-Securing Declaration**: We have not been suspended nor declared ineligible by the Procuring Agency based on execution of a Bid Securing Declaration or Proposal Securing Declaration in the Procuring Agency's country in accordance with ITB 4;
(d) **Conformity:** We offer to supply in conformity with the bidding document and in accordance with the Delivery Schedules specified in the Schedule of Requirements the following Goods: [*insert a brief description of the Goods and Related Services*];
(e) **Bid Validity Period**: Our Bid shall be valid for the period specified in **BDS 17.1** (as amended, if applicable) from the date fixed for the Bid submission deadline specified in **BDS 23.1** (as amended, if applicable), and it shall remain binding upon us, and may be accepted at any time before the expiration of that period;
(f) **Performance Security**: If our Bid is accepted, we commit to obtain a performance security in accordance with the bidding document;
(g) **One Bid per Bidder**: We are not submitting any other Bid(s) as an individual Bidder, and we are not participating in any other bid(s) as a Joint Venture member or as a subcontractor, and meet the requirements, other than Alternative Bids submitted in accordance with **ITB 19**;
(h) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the Procuring Agency. Further, we are not ineligible under Pakistan laws;

(i) **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 but meet the requirements of*];

(j) **Binding Contract**: We understand that this Bid, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

(k) **Not Bound to Accept**: We understand that you are not bound to accept the Most Advantageous Bid or any other Bid that you may receive; and

(l) **Fraud and Corruption**: We hereby certify that we have taken steps to ensure that no person acting for us, or on our behalf, engages in any type of Fraud and Corruption.

Name of the Bidder: *[*insert complete name of Bidder*]

Name of the person duly authorized to sign the Bid on behalf of the Bidder: ** [*insert complete name of person duly authorized to sign the Bid*]

Title of the person signing the Bid: [*insert complete title of the person signing the Bid*]

Signature of the person named above: [*insert signature of person whose name and capacity are shown above*]

Date signed [*insert date of signing*] **day of** [*insert month*], [*insert year*]

*: In the case of the Bid submitted by a Joint Venture specify the name of the Joint Venture as Bidder.
**: Person signing the Bid shall have the power of attorney given by the Bidder. The power of attorney shall be attached with the Bid Schedules.

Form 1 (B) Letter of Bid For Financial Proposal

INSTRUCTIONS TO BIDDERS: (delete this box once you have completed the document)

*Place this Letter of Bid in the **second envelope "FINANCIAL PROPOSAL".***

The Bidder must prepare the Letter of Bid on stationery with its letterhead clearly showing the Bidder's complete name and business address.

Note: All italicized text in black font is to help Bidders in preparing this form and Bidders shall delete it from the final document.

Date of this Bid submission: [*insert date (as day, month and year) of Bid submission*]
RFB No.: [*insert number of bidding process*]
Request for Bid No.: [*insert identification*]

We, the undersigned Bidder, hereby submit our Bid, in two parts, namely:

(a) the Technical Proposal, and
(b) the Financial Proposal.

In submitting our Bid we make the following declarations:

(a) **No reservations:** We have examined and have no reservations to the bidding document, including addenda issued in accordance with Instructions to Bidders (ITB 9);
(b) **Eligibility**: We meet the eligibility requirements and have no conflict of interest in accordance with ITB 3;
(c) **Bid/Proposal-Securing Declaration**: We have not been suspended nor declared ineligible by the Procuring Agency based on execution of a Bid Securing Declaration or Proposal Securing Declaration in the Procuring Agency's country in accordance with ITB 4;
(d) **Conformity:** We offer to supply in conformity with the bidding document and in accordance with the Delivery Schedules specified in the Schedule of Requirements the following Goods: [*insert a brief description of the Goods and Related Services*];
(e) **Total Price:** The total price of our Bid, excluding any discounts offered in item (c) below is:

In case of only one lot, the total price of the Bid is [*insert the total price of the bid in words and figures, indicating the various amounts and the respective currencies*];

In case of multiple lots, the total price of each lot is [*insert the total price of each lot in words and figures, indicating the various amounts and the respective currencies*];

In case of multiple lots, total price of all lots (sum of all lots) [*insert the total price of all lots in words and figures, indicating the various amounts and the respective currencies*];

(f) **Discounts:** The discounts offered and the methodology for their application are:

(i) The discounts offered are: [*Specify in detail each discount offered*]

(ii) The exact method of calculations to determine the net price after application of discounts is shown below: [*Specify in detail the method that shall be used to apply the discounts*];

(g) **Bid Validity Period**: Our Bid shall be valid for the period specified in **BDS 17.1** (as amended, if applicable) from the date fixed for the Bid submission deadline specified in **BDS 23.1** (as amended, if applicable), and it shall remain binding upon us, and may be accepted at any time before the expiration of that period;

(h) **Performance Security**: If our Bid is accepted, we commit to obtain a performance security in accordance with the bidding document;

(i) **One Bid per Bidder**: We are not submitting any other Bid(s) as an individual Bidder, and we are not participating in any other bid(s) as a Joint Venture member or as a subcontractor, and meet the requirements, other than Alternative Bids submitted in accordance with **ITB 19**;

(j) **Suspension and Debarment**: We, along with any of our subcontractors, suppliers, consultants, manufacturers, or service providers for any part of the contract, are not subject to, and not controlled by any entity or individual that is subject to, a temporary suspension or a debarment imposed by the Procuring Agency. Further, we are not ineligible under Pakistan laws;

(k) **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 but meet the requirements of*];

(l) **Binding Contract**: We understand that this Bid, together with your written acceptance thereof included in your Letter of Acceptance, shall constitute a binding contract between us, until a formal contract is prepared and executed;

(m) **Not Bound to Accept**: We understand that you are not bound to accept the Most Advantageous Bid or any other Bid that you may receive; and

(n) **Fraud and Corruption**: We hereby certify that we have taken steps to ensure that no person acting for us, or on our behalf, engages in any type of Fraud and Corruption.

Name of the Bidder: *[*insert complete name of Bidder*]

Name of the person duly authorized to sign the Bid on behalf of the Bidder: ** [*insert complete name of person duly authorized to sign the Bid*]

Title of the person signing the Bid: [*insert complete title of the person signing the Bid*]

Signature of the person named above: [*insert signature of person whose name and capacity are shown above*]

Date signed [*insert date of signing*] **day of** [*insert month*], [*insert year*]

*: In the case of the Bid submitted by a Joint Venture specify the name of the Joint Venture as Bidder.
**: Person signing the Bid shall have the power of attorney given by the Bidder. The power of attorney shall be attached with the Bid Schedules.

Bidder Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]

Date: *[insert date (as day, month and year) of bid submission*]
No.: *[insert number of bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

Page__of____pages

1. Bidder's Name *[insert Bidder's legal name]*
2. In case of JV, legal name of each member : *[insert legal name of each member in JV]*
3. Bidder's actual or intended country of registration: *[insert actual or intended country of registration]*
4. Bidder's year of registration: *[insert Bidder's year of registration]*
5. Bidder's Address in country of registration: *[insert Bidder's legal address in country of registration]*
6. Bidder's Authorized Representative Information Name: *[insert Authorized Representative's name]* Address: *[insert Authorized Representative's Address]* Telephone/Fax numbers: *[insert Authorized Representative's telephone/fax numbers]* Email Address: *[insert Authorized Representative's email address]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* Articles of Incorporation (or equivalent documents of constitution or association), and/or documents of registration of the legal entity named above. In case of JV, letter of intent to form JV or JV agreement, in accordance with ITB 3.4. Establishing that the Bidder is not under the supervision of the Procuring Agency 8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

Bidder's JV Members Information Form

[The Bidder shall fill in this Form in accordance with the instructions indicated below. The following table shall be filled in for the Bidder and for each member of a Joint Venture]].
Date: *[insert date (as day, month and year) of Bid submission*]
RFB No.: *[insert number of RFB process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

Page__of____pages

1. Bidder's Name: *[insert Bidder's legal name]*
2. Bidder's JV Member's name: *[insert JV's Member legal name]*
3. Bidder's JV Member's country of registration: *[insert JV's Member country of registration]*
4. Bidder's JV Member's year of registration: *[insert JV's Member year of registration]*
5. Bidder's JV Member's legal address in country of registration: *[insert JV's Member legal address in country of registration]*
6. Bidder's JV Member's authorized representative information Name: *[insert name of JV's Member authorized representative]* Address: *[insert address of JV's Member authorized representative]* Telephone/Fax numbers: *[insert telephone/fax numbers of JV's Member authorized representative]* Email Address: *[insert email address of JV's Member authorized representative]*
7. Attached are copies of original documents of *[check the box(es) of the attached original documents]* Articles of Incorporation (or equivalent documents of constitution or association), and/or registration documents of the legal entity named above, in accordance with ITB 4.4. 8. Included are the organizational chart, a list of Board of Directors, and the beneficial ownership.

Form of Qualification Information

1. Individual Bidders or Individual Members of Joint Ventures

Constitution or legal status of Bidder: *[attach copy]*

Place of registration: *[insert]*

Principal place of business: *[insert]*

Power of attorney of signatory of Bid: *[attach]*

Total annual volume of Supplies delivered *(insert period)* years, in the internationally traded currency specified in the Bid Data Sheet: *[insert]*

Services performed as prime Supplier on the provision of Services of a similar nature and volume over the last *(insert period)* years. The values should be indicated in the same currency used for Item 1.2 above. Also list details of work under way or committed, including expected completion date.

Project name and country	Name of PA and contact person	Type of Supplies provided and year of completion	Value of Contract
(a) (b)			

Major items of Supplier's Equipment proposed for carrying out the Services. List all information requested below. Refer also to ITB 13.3(c).

Item of equipment	Description, make, and age (years)	Condition (new, good, poor) and number available	Owned, leased (from whom?), or to be purchased (from whom?)

(a) (b)			

Qualifications and experience of key personnel proposed for administration and execution of the Contract. Attach biographical data. Refer also to ITB 13.3(d).

Position	Name	Years of experience (general)	Years of experience in proposed position
(a) (b)			

Proposed sub-contracts and firms involved. Refer to GCC 18.

Sections of the Services	Value of Sub-contract	Sub-contractor (name and address)	Experience in providing similar Services
(a) (b)			

Financial reports for the last *(insert period)* years: balance sheets, profit and loss statements, auditors' reports, etc. List below and attach copies.

Evidence of access to financial resources to meet the qualification requirements: cash in hand, lines of credit, etc. List below and attach copies of support documents. We certify/confirm that we comply with eligibility requirements as per ITB 3 of the bidding documents.

Name, address, and telephone, telex, and facsimile numbers of banks that may provide references if contacted by the Procuring Agency.

Information regarding any litigation, current or within the last *(insert period)* years, in which the Bidder is or has been involved.

Other party(ies)	Cause of dispute	Details of litigation award	Amount involved
(a) (b)			

Information regarding Occupation Health and Safety Policy and Safety Records of the Bidder.

Statement of compliance with the requirements of ITB 3.4.

1.13 Proposed Program (service work method and schedule). Descriptions, drawings, and charts, as necessary, to comply with the requirements of the bidding documents.

2. Joint Ventures

The information listed in 1.11 - 1.12 above shall be provided for each members of the joint venture.

The information in 1.13 above shall be provided for the joint venture.

Attach the power of attorney of the signatory (ies) of the Bid authorizing signature of the Bid on behalf of the joint venture.

Attach the Contract among all members of the joint venture (and which is legally binding on all members), which shows that

all members shall be jointly and severally liable for the execution of the Contract in accordance with the Contract terms;

one of the members will be nominated as being in-charge, authorized to incur liabilities, and receive instructions for and on behalf of any and all members of the joint venture; and

the execution of the entire Contract, including payment, shall be done exclusively with the member in charge.

3. Additional Requirements

3.1 Bidders should provide any additional information required in the Bid Data Sheet and to fulfill the requirements of ITB 12.1, if applicable.

We, the undersigned declare that

The information contained in and attached to this form is true and accurate as of the date of bid submission

Or [delete statement which does not apply]

The originally submitted pre-qualification information remains essentially correct as of date of submission

Authorized Signature:

Name and Title of Signatory:

Name of Bidder: _____

Address: _____

Form FIN

Financial Situation and Performance

[The following table shall be filled in for the Bidder and for each member of a Joint Venture]

Bidder's Name: *[insert full name]*
Date: *[insert day, month, year]* Joint Venture Member Name: *[insert full name]* RFB No. and title: *[insert RFB number and title]*
Page *[insert page number]* of *[insert total number]* pages

1. Financial data

Type of Financial information in (currency)	**Historic information for previous _***[insert number] years, [insert in words]* **(amount in currency, currency, exchange rate,)**				
	Year 1	Year 2	Year 3		
Statement of Financial Position (Information from Balance Sheet)					
Total Assets (TA)					
Total Liabilities (TL)					
Total Equity/Net Worth (NW)					
Current Assets (CA)					
Current Liabilities (CL)					
Working Capital (WC)					
Information from Income Statement					
Total Revenue (TR)					
Profits Before Taxes (PBT)					
Cash Flow Information					
Cash Flow from Operating Activities					

2. Financial documents

The Bidder and its parties shall provide copies of financial statements for *[number]* years pursuant Section III, Qualifications Criteria and Requirements, Sub-factor 3.1. The financial statements shall:

(a) reflect the financial situation of the Bidder or in case of JV member, and not an affiliated entity (such as parent company or group member).

(b) be independently audited or certified in accordance with local legislation.

(c) be complete, including all notes to the financial statements.

(d) correspond to accounting periods already completed and audited.

☐ Attached are copies of financial statements for the *[number]* years required above; and complying with the requirements.

Average Annual Turnover (Annual Sales Value)

[The following table shall be filled in for the Bidder and for each member of a Joint Venture]

Bidder's Name: *[insert full name]*
Date: *[insert day, month, year]* Joint Venture Member Name: *[insert full name]* RFB No. and title: *[insert RFB number and title]*
Page *[insert page number]* of *[insert total number]* pages

Annual turnover data		
Year	**Exchange rate** **Currency**	**PKR equivalent**
[indicate calendar year]	*[indicate currency]*	
	Average Annual Turnover *	

* Total PKR equivalent for all years divided by the total number of years.

Price Schedule Forms

[The Bidder shall fill in these Price Schedule Forms in accordance with the instructions indicated. In TBML systems procurement, the Contract Price (and payment schedule) should be linked as much as possible to achievement of operational capabilities, not just to the physical delivery of technology

Preamble:

Procuring agency should highlight any special requirements of the TBML System and Contract in a Preamble to the Price Schedules. The following is an example of one such preamble;

1. The Price Schedules are divided into separate Schedules as follows:
   i. Supply and Installation Cost Sub-Table(s)
   ii. Recurrent Cost Sub-Tables(s)
   iii. Grand Summary Cost Table
   iv. *[insert: **any other Schedules as appropriate**]*
2. The Schedules do not generally give a full description of the information technologies to be supplied, installed, and operationally accepted, or the Services to be performed under each item. However, it is assumed that Bidders shall have read the Technical Requirements and other sections of these Bidding Documents to ascertain the full scope of the requirements associated with each item prior to filling in the rates and prices. The quoted rates and prices shall be deemed to cover the full scope of these Technical Requirements, as well as overhead and profit.
3. If Bidders are unclear or uncertain as to the scope of any item, they shall seek clarification in accordance with the Instructions to Bidders in the Bidding Documents prior to submitting their bid.

Pricing

4. Prices shall be filled in indelible ink, and any alterations necessary due to errors, etc., shall be initialed by the Bidder. As specified in the Bid Data Sheet, prices shall be fixed and firm for the duration of the Contract.
5. Bid prices shall be quoted in the manner indicated and in the currencies specified in ITB Clauses 15. Prices must correspond to items of the scope and quality defined in the Technical Requirements or elsewhere in these Bidding Documents.
6. The Bidder must exercise great care in preparing its calculations, since there is no opportunity to correct errors once the deadline for submission of bids has passed. A single error in specifying a unit price can therefore change a Bidder's overall total bid price substantially, make the bid noncompetitive, or subject the Bidder to possible loss. The Procuring Agency will correct any arithmetic error.
7. Payments will be made to the Supplier in the currency or currencies indicated under each respective item. As specified in ITB Clause 15.1 (ITB Clause 28.1 in the two-stage SBD), no more than three foreign currencies may be used. The price of an item should be unique regardless of installation site.

Supply and Installation Cost Table

As necessary for supply, installation, and achieving Operational Acceptance of the System, specify items in the Table below, modifying, deleting, or expanding the sample line items and sample table entries as needed. Costs MUST reflect prices and rates quoted in accordance with ITB Clauses 14 and 15.

				Unit Prices / Rates			**Total Prices**		
				Supplied Locally	**Supplied from Abroad**		**Supplied Locally**	**Supplied from Abroad**	
Compo-nent No.	**Component Description**	**Country of Origin Code**	**Quantity**	***[insert: local currency]***	***[insert: local currency]***	***[insert: foreign currency A]***	***[insert: local currency]***	***[insert: local currency]***	***[insert: foreign currency A]***
Subtotals (to *[insert:* ***line item***] of Supply and Installation Cost Summary Table)									

Note: - - indicates not applicable.

Name of Bidder:	
Authorized Signature of Bidder:	

Recurrent Cost Sub-Table [insert: identifying number]

The detailed components and quantities in the Sub-Table below for the line item specified above, modifying the sample components and sample table entries as needed. *Repeat the Sub-Table as needed to cover each and every line item in the Recurrent Cost Summary Table that requires elaboration.* Costs MUST reflect prices and rates quoted in accordance with ITB Clauses 14 and 15.

		Maximum all-inclusive costs (for costs in *[insert: **currency**]*)						
Component No.	Component	Y1	Y2	Y3	Y4	...	Yn	Sub-total for *[insert: **currency**]*
	Annual Subtotals:							
Cumulative Subtotal (to *[insert: **currency**]* entry for *[insert: **line item**]* in the Recurrent Cost Summary Table)								

Name of Bidder:	
Authorized Signature of Bidder:	

Note: The cost for maintenance must be quoted after expiry of the warranty period e.g. if a component is having three year warranty than the price charged for such maintenance shall be applicable after expiry of the warranty period.

Grand Summary Cost Table

[	*insert:* ***Local Currency*** *]* Price	*[insert:* ***Foreign Currency*** Price
1. Supply and Installation Costs		
2. Recurrent Costs		
3. Grand Totals (to Bid Submission Form)		

Name of Bidder:	
Authorized Signature of Bidder:	

Manufacturer's Authorization

*[The Bidder shall require the Manufacturer to fill in this Form in accordance with the instructions indicated. This letter of authorization should be on the letterhead of the Manufacturer and should be signed by a person with the proper authority to sign documents that are binding on the Manufacturer. The Bidder shall include it in its Bid, if so indicated in the **BDS.**]*

Date: *[insert date (as day, month and year) of Bid submission]*
No.: *[insert number of bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

To: *[insert complete name of Procuring Agency]*

WHEREAS

We *[insert complete name of Manufacturer],* who are official manufacturers of *[insert type of product],* having factories at [insert full address of Manufacturer's factories], do hereby authorize *[insert complete name of Bidder]* (hereinafter, the "Bidder") to submit a bid and subsequently negotiate and sign a Contract with you for resale of the following Products produced by us:
We hereby extend our full guarantee and warranty in accordance with Clause 29 of the General Conditions of Contract, with respect to the Therapeutic Goods offered by the above firm.

Signed: *[insert signature(s) of authorized representative(s) of the Manufacturer]*

Name: *[insert complete name(s) of authorized representative(s) of the Manufacturer]*

Title: *[insert title]*

Dated on_____day of_,_____*[insert date of signing]*

Software List

	(select one per item)			(select one per item)	
Software Item	System Software	General-Purpose Software	Application Software	Standard Software	Custom Software

General Information Form

All individual firms and each partner of a Joint Venture that are bidding must complete the information in this form. Nationality information should be provided for all owners or Bidders that are partnerships or individually owned firms.

Where the Bidder proposes to use named Subcontractors for highly specialized components of the TBML System, the following information should also be supplied for the Subcontractor(s).

1.	Name of firm	
2.	Head office address	
3.	Telephone	Contact
4.	Fax	Telex
5.	Place of incorporation / registration	Year of incorporation / registration

Nationality of beneficial owners along with shares percentage			
Name		Nationality	Share Percentage
1.			
2.			
3.			
4.			
5.			
To be completed by all owners of partnerships or individually owned firms.			

List of Proposed Sub Contractors

	Item	Proposed Subcontractor	Place of Registration & Qualifications

Details of Contracts of Similar Nature and Complexity

Name of Bidder or partner of a Joint Venture

Use a separate sheet for each contract.

1.	Number of contract	
	Name of contract	
	Country	
2.	Name of Procuring Agency	
3.	Procuring Agency address	
4.	Nature of TBML Systems and special features relevant to the contract for which the Bidding Documents are issued	
5.	Contract role (check one) ☐Prime Supplier ☐ Management Contractor ☐ Subcontractor ☐ Partner in a Joint Venture	
6.	Amount of the total contract/subcontract/partner share (in specified currencies at completion, or at date of award for current contracts) Currency Currency Currency	
7.	Equivalent amount PKR Total contract: ___; Subcontract: _____; Partner share: _____;	
8.	Date of award/completion	
9.	Contract was completed _____ months ahead/behind original schedule (if behind, provide explanation).	
10.	Contract was completed PKR _____ equivalent under/over original contract amount (if over, provide explanation).	
11.	Special contractual/technical requirements.	
12.	Indicate the approximate percent of total contract value (and PKR amount) of TBML System undertaken by subcontract, if any, and the nature of such TBML System.	

Form of Bid Security

[The bank shall fill in this Bank Guarantee Form in accordance with the instructions indicated.]

[Guarantor letterhead or SWIFT identifier code]

Beneficiary: *[Procuring Agency to insert its name and address]*

No.: *[Procuring Agency to insert reference number for the Request for Bids]*

Alternative No.: *[Insert identification No if this is a Bid for an alternative]*

Date: *[Insert date of issue]*

BID GUARANTEE No.: *[Insert guarantee reference number]*

Guarantor: *[Insert name and address of place of issue, unless indicated in the letterhead]*

We have been informed that _____ *[insert name of the Bidder, which in the case of a joint venture shall be the name of the joint venture (whether legally constituted or prospective) or the names of all members thereof]* (hereinafter called "the Applicant") has submitted or will submit to the Beneficiary its Bid (hereinafter called "the Bid") for the execution of _____ under Request for Bids No. _____ _ ("the RFB").

Furthermore, we understand that, according to the Beneficiary's conditions, Bids must be supported by a Bid guarantee.

At the request of the Applicant, we, as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of _____ (_____) upon receipt by us of the Beneficiary's complying demand, supported by the Beneficiary's statement, whether in the demand itself or a separate signed document accompanying or identifying the demand, stating that either the Applicant:

(a) has withdrawn its Bid during the period of Bid validity set forth in the Applicant's Letter of Bid ("the Bid Validity Period"), or any extension thereto provided by the Applicant; or

(b) having been notified of the acceptance of its Bid by the Beneficiary during the Bid Validity Period or any extension thereto provided by the Applicant, (i) has failed to sign the contract agreement, or (ii) has failed to furnish the performance security, in accordance with the Instructions to Bidders ("ITB") of the Beneficiary's bidding document.

This guarantee will expire: (a) if the Applicant is the successful Bidder, upon our receipt of copies of the Contract agreement signed by the Applicant and the performance security issued to the Beneficiary in relation to such Contract agreement; or (b) if the Applicant is not the successful Bidder, upon the earlier

of (i) our receipt of a copy of the Beneficiary's notification to the Applicant of the results of the Bidding process; or (ii) twenty-eight days after the end of the Bid Validity Period.

Consequently, any demand for payment under this guarantee must be received by us at the office indicated above on or before that date.

_____

[Signature(s)]

Note: All italicized text is for use in preparing this form and shall be deleted from the final product.

Form of Bid-Securing Declaration

[The Bidder shall fill in this Form in accordance with the instructions indicated.]

Date: *[date (as day, month and year)]*
No.: *[number of bidding process]*
Alternative No.: *[insert identification No if this is a Bid for an alternative]*

To: *[complete name of Procuring Agency]*

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid-Securing Declaration.

We accept that we will be blacklisted and henceforth cross debarred for participating in respective category of public procurement proceedings for a period of (not more than) six months, if fail to abide with a bid securing declaration, however without indulging in corrupt and fraudulent practices, if we are in breach of our obligation(s) under the Bid conditions, because we:

(a) have withdrawn our Bid during the period of Bid validity specified in the Letter of Bid; or

(b) having been notified of the acceptance of our Bid by the Procuring Agency during the period of Bid validity, (i) fail or refuse to sign the Contract; or (ii) fail or refuse to furnish the Performance Security (or guarantee), if required, in accordance with the ITB.

We understand this Bid Securing Declaration shall expire if we are not the successful Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight days after the expiration of our Bid.

Name of the Bidder*****_____

Name of the person duly authorized to sign the Bid on behalf of the Bidder******_____

Title of the person signing the Bid_____

Signature of the person named above_____

Date signed _____ day of _____, _____

*****: In the case of the Bid submitted by joint venture specify the name of the Joint Venture as Bidder
******: Person signing the Bid shall have the power of attorney given by the Bidder attached to the Bid

[Note: In case of a Joint Venture, the Bid-Securing Declaration must be in the name of all members to the Joint Venture that submits the Bid.]

Letter of Acceptance

[Letter head paper of the Procuring Agency]

[date]

To: [name and address of the Supplier]

This is to notify you that your Bid dated [date] for execution of the [name of the Contract and identification number, as given in the Special Conditions of Contract] for the Contract Price of the equivalent of [amount in numbers and words] [name of currency], as corrected and modified in accordance with the Instructions to Bidders is hereby accepted by us.

We hereby confirm [insert the name of the Appointing Authority], to be the Appointing Authority, to appoint the Arbitrator in case of any arisen disputes.

You are hereby informed that after you have read and return the attached draft Contract the parties to the contract shall sign the vetted contract within fourteen (14) working days.

You are hereby required to furnish the Performance Guarantee/Security in the form and the amount stipulated in the Special Conditions of the Contract within a period of fourteen (14) days after the receipt of Letter of Acceptance.

Authorized Signature:

Name and Title of Signatory:

Name of Agency:

Attachment: Contract

Copy: Appointing Authority and Supplier

SECTION VII: GENERAL CONDITIONS OF THE CONTRACT

GENERAL CONDITIONS OF THE CONTRACT (GCC)

1.	Definitions	1.1	The following words and expressions shall have the meanings hereby assigned to them:	
			a)	"**Authority**" means Public Procurement Regulatory Authority.
			b)	The "**Arbitrator**" is the person appointed with mutual consent of both the parties, to resolve contractual disputes as provided for in the General Conditions of the Contract **GCC Clause 45** hereunder.
			c)	The "**Contract**" means the agreement entered into between the Procuring Agency and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.
			d)	The "**Commencement Date**" is the date when the Supplier shall commence execution of the contract as specified in the **SCC**.
			e)	"**Completion**" means the fulfillment of the related services by the Supplier in accordance with the terms and conditions set forth in the contract.
			f)	"**Country of Origin**" means the countries and territories eligible under the PPRA Rules 2004 and its corresponding Regulations as further elaborated in the **SCC**.
			g)	The "**Contract Price**" is the price stated in the Letter of Acceptance and thereafter as adjusted in accordance with the provisions of the Contract.
			h)	"**Effective Contract date**" is the date shown in the Certificate of Contract Commencement issued by the Procuring Agency upon fulfillment of the conditions precedent stipulated in **GCC Clause 5**.
			i)	"**Procuring Agency**" means the person named as Procuring Agency in the **SCC** and the legal successors in title to this person, procuring the Goods and related service, as named in
			j)	"**Related Services**" means those services ancillary to the delivery of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, initial maintenance and other such obligations of the
			k)	"**GCC**" means the General Conditions of Contract contained in this section.

			l)	"**Intended Delivery Date**" is the date on which it is intended that the Supplier shall effect delivery as specified in the **SCC**.
			m)	"**TBML System**," also called "the System," means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational (exclusive of the Supplier's Equipment), together with the Services to be carried out by the Supplier under the Contract
			n)	"**SCC**" means the Special Conditions of Contract.
			o)	"**Supplier**" means the individual private or government entity or a combination of the above whose Bid to perform the contract has been accepted by the Procuring Agency and is named as such in the Contract Agreement, and includes the legal successors or permitted assigns of the supplier and shall
			p)	**"Project Name"** means the name of the project stated in **SCC**.
			q)	"**Day**" means calendar day.
			r)	"**Eligible Country**" means the countries and territories eligible for participation in accordance with the policies of the Federal Government.
			s)	"**End User**" means the organization(s) where the goods will be used, as named in the **SCC**.
			t)	"**Origin**" means the place where the Goods were mined, grown, or produced or from which the Services are supplied. Goods are produced when, through manufacturing, processing, or substantial and major assembly of components, a commercially recognized new produce results that is substantially different in basic characteristics or in purpose or utility from its components.
			u)	"**Force Majeure**" means an unforeseeable event which is beyond reasonable control of either Party and which makes a Party's performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances. For the purposes of this Contract, "**Force Majeure**" means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of a Party, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the

				circumstances. and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood, epidemics, or other adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent), confiscation or any other action by Government agencies.
			v)	"**Specification**" means the Specification of the Goods and performance of incidental services in accordance with the relevant standards included in the Contract and any modification or addition made or approved by the Procuring Agency.
			w)	The Supplier's Bid is the completed Bid document submitted by the Supplier to the Procuring Agency.
2.	**Application and interpretation**	2.1		These General Conditions shall apply to the extent that they are not superseded by provisions of other parts of the Contract.
		2.2		In interpreting these Conditions of Contract headings and marginal notes are used for convenience only and shall not affect their interpretations unless specifically stated; references to singular include the plural and vice versa; and masculine include the feminine. Words have their ordinary meaning under the language of the Contract unless specifically defined.

		2.3	The documents forming the Contract shall be interpreted in the following order of priority: Form of Contract, Special Conditions of Contract, General Conditions of Contract, Letter of Acceptance, Certificate of Contract Commencement Specifications Contractor's Bid, and Any other document listed in the Special Conditions of Contract as forming part of the Contract.
3.	**Conditions Precedent**	3.1	Having signed the Contract, it shall come into effect on the date on which the following conditions have been satisfied: - Submission of performance Security (or guarantee) in the form specified in the **SCC**; Furnishing of Advance Payment Unconditional Guarantee.
		3.2	If the Condition precedent stipulated on GCC Clause 3.1 is not met by the date specified in the SCC this contract shall not come into effect;
		3.3	If the Procuring Agency is satisfied that each of the conditions precedent in this contract has been satisfied (except to the extent waved by him, but subject to such conditions as he shall impose in respect of such waiver) he shall promptly issue to the supplier a certificate of Contract commencement, which shall confirm the start date.
4.	**Governing Language**	4.1	The Contract as all correspondence and documents relating to the contract exchanged by the Supplier and the Procuring Agency shall be written in the language specified in **SCC**. Subject to **GCC Clause 3.1**, the version of the Contract written in the specified language shall govern its interpretation.
5.	**Applicable Law and Effectiveness of the contract**	5.1	The contract shall be governed and interpreted in accordance with the laws of Pakistan, unless otherwise specified in SCC.

		5.2	The Contract shall be effective from the date specified in the SCC,
6.	**Country of Origin**	6.1	The origin of goods and services makingTBML systems may be distinct from the nationality of the Supplier.
7.	**Scope of the TBMLSystem**	7.1	Unless otherwise expressly limited in the SCC or Technical Requirements, the Supplier's obligations cover the provision of all Information Technologies, Materials and other Goods as well as the performance of all Services required for the design, development, and implementation (including procurement, quality assurance, assembly, associated site preparation, Delivery, Pre-commissioning, Installation, Testing, and Commissioning) of the System, in accordance with the plans, procedures, specifications, drawings, codes, and any other documents specified in the Contract and the Agreed and Finalized Project Plan
		7.2	The Supplier shall, unless specifically excluded in the Contract, perform all such work and / or supply all such items and Materials not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining Operational Acceptance of the System as if such work and / or items and Materials were expressly mentioned in the Contract.
		7.3	The Supplier's obligations (if any) to provide Goods and Services as implied by the Recurrent Cost tables of the Supplier's bid, such as consumables, spare parts, and technical services (e.g., maintenance, technical assistance, and operational support), are as specified in the SCC, including the relevant terms, characteristics, and timings
8.	**Supplier's Responsibilities**	8.1	The Supplier shall conduct all activities with due care and diligence, in accordance with the Contract and with the skill and care expected of a competent provider of information technologies, TBML systems, support, maintenance, training, and other related services, or in accordance with best industry practices. In particular, the Supplier shall provide and employ only technical personnel who are skilled and experienced in their respective callings and supervisory staff who are competent to adequately supervise the work at hand.

		8.2	The Supplier confirms that it has entered into this Contract on the basis of a proper examination of the data relating to the System provided by the Procuring agency and on the basis of information that the Supplier could have obtained from a visual inspection of the site (if access to the site was available) and of other data readily available to the Supplier relating to the System as at the date Seven (07) days prior to bid submission. The Supplier acknowledges that any failure to acquaint itself with all such data and information shall not relieve its responsibility for properly estimating the difficulty or cost of successfully performing the Contract
		8.3	The Supplier shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach a mutually Agreed and Finalized Project Plan within the time schedule specified in the Implementation Schedule in the Technical Requirements Section. Failure to provide such resources, information, and decision making may constitute grounds for termination.
		8.4	The Supplier shall acquire in its name all permits, approvals, and/or licenses from all local, state, or national government authorities or public service undertakings in the Procuring agency's Country that are necessary for the performance of the Contract, including, without limitation, visas for the Supplier's and Subcontractor's personnel and entry permits for all imported Supplier's Equipment. The Supplier shall acquire all other permits, approvals, and/or licenses that are not the responsibility of the Procuring agency and that are necessary for the performance of the Contract.
		8.5	The Supplier shall comply with all laws in force in the Procuring agency's Country. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract and are binding upon the Supplier. The Supplier shall indemnify and hold harmless the Procuring agency from and against any and all liabilities, damages, claims, fines, penalties, and expenses of whatever nature arising or resulting from the violation of such laws by the Supplier or its personnel, including the Subcontractors and their personnel, but without prejudice to GCC Clause 9.1. The Supplier shall not indemnify the Procuring agency to the extent that such liability, damage, claims, fines, penalties, and expenses were caused or contributed to by a fault of the Procuring agency.

		8.6	The Supplier shall, in all dealings with its labor and the labor of its Subcontractors currently employed on or connected with the Contract, pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations pertaining to the employment of labor.
		8.7	Any Information Technologies or other Goods and Services that will be incorporated in or be required for the System and other supplies shall have their Origin in a country that shall be an Eligible Country.
		8.8	The Supplier shall permit the Procuring Agency and/or persons appointed by the Procuring Agency to inspect the Supplier's offices and/or the accounts and records of the Supplier and its sub-contractors relating to the performance of the Contract, and to have
		8.9	Other Supplier responsibilities, if any, are as stated in the SCC.
9.	**Procuring Agency's Responsibility**	9.1	The Procuring Agency shall ensure the accuracy of all information and/or data to be supplied by the Procuring agency to the Supplier, except when otherwise expressly stated in the Contract.
		9.2	The Procuring agency shall be responsible for timely provision of all resources, information, and decision making under its control that are necessary to reach an Agreed and Finalized Project Plan (pursuant to **GCC Clause 17**) within the time schedule specified in the Implementation Schedule in the Technical Requirements Section. Failure to provide such resources, information, and decision making may constitute grounds for Termination pursuant to **GCC Clause 41.**
		9.3	The Procuring agency shall be responsible for acquiring and providing legal and physical possession of the site and access to it, and for providing possession of and access to all other areas reasonably required for the proper execution of the Contract.
		9.4	If requested by the Supplier, the Procuring agency shall use its best endeavors to assist the Supplier in obtaining in a timely and expeditious manner all permits, approvals, and/or licenses necessary for the execution of the Contract from all local, state, or national government authorities or public service undertakings that such authorities or undertakings require the Supplier or Subcontractors or the personnel of the Supplier or Subcontractors, as the case may be, to obtain.

		9.5	In such cases where the responsibilities of specifying and acquiring or upgrading telecommunications and/or electric power services falls to the Supplier, as specified in the Technical Requirements, SCC, Agreed and Finalized Project Plan, or other parts of the Contract, the Procuring agency shall use its best endeavors to assist the Supplier in obtaining such services in a timely and expeditious manner.
		9.6	The Procuring agency shall be responsible for timely provision of all resources, access, and information necessary for the Installation and Operational Acceptance of the System (including, but not limited to, any required telecommunications or electric power services), as identified in the Agreed and Finalized Project Plan, except where provision of such items is explicitly identified in the Contract as being the responsibility of the Supplier. Delay by the Procuring agency may result in an appropriate extension of the Time for Operational Acceptance, at the Supplier's discretion
		9.7	Unless otherwise specified in the Contract or agreed upon by the Procuring agency and the Supplier, the Procuring agency shall provide sufficient, properly qualified operating and technical personnel, as required by the Supplier to properly carry out Delivery, Pre- commissioning, Installation, Commissioning, and Operational Acceptance, at or before the time specified in the Technical Requirements Section's Implementation Schedule and the Agreed and Finalized Project Plan.
		9.8	The Procuring agency will designate appropriate staff for the training courses to be given by the Supplier and shall make all appropriate logistical arrangements for such training as specified in the Technical Requirements, SCC, the Agreed and Finalized Project Plan, or other parts of the Contract.
		9.9	The Procuring agency assumes primary responsibility for the Operational Acceptance Test(s) for the System, in accordance with GCC Clause 26, and shall be responsible for the continued operation of the System after Operational Acceptance. However, this shall not limit in any way the Supplier's responsibilities after the date of Operational Acceptance otherwise specified in the Contract.
		9.10	The Procuring agency is responsible for performing and safely storing timely and regular backups of its data and Software in accordance with accepted data management principles, except where such responsibility is clearly assigned to the Supplier elsewhere in the Contract.

		9.11	Other Procuring agency responsibilities, if any, are as stated in the SCC.
10.	**Prices**	10.1	The contract price shall be as specified in the Contract Agreement Subject to any additions and adjustments thereto or deductions there from, as may be made pursuant to the Contract.
		10.2	Prices charged by the Supplier for TBML System under the Contract shall not vary from the prices quoted by the Supplier in its Bid, with the exception of any price adjustments authorized in SCC or in the Procuring Agency's request for Bid Validity extension, as the case may be.
11.	**Payment**	11.1	The method and conditions of payment to be made to the Supplier under this Contract shall be specified in SCC.
		11.2	The Supplier's request(s) for payment shall be made to the Procuring Agency in writing or in electronic forms that provide record of the content of communication, accompanied by an invoice describing, as appropriate, the Goods delivered and Services performed, and by documents submitted, and upon fulfillment of other obligations stipulated in the Contract.
		11.3	Payments shall be made promptly by the Procuring Agency, within sixty (60) days after submission of an invoice or claim by the Supplier. If the Procuring Agency makes a late payment, the Supplier shall be paid interest on the late payment. Interest shall be calculated from the date by which the payment should have been made up to the date when the late payment is made at the rate as specified in the **SCC**.
		11.4	The currency or currencies in which payment is made to the Supplier under this Contract shall be specified in **SCC** subject to the following general principle: payment will be made in the currency or currencies in which the payment has been requested in the Supplier's Bid.
		11.5	All payments shall be made in the currency or currencies specified in the **SCC** pursuant to **GCC Clause 11.4**
12.	**Performance Guarantee**	12.1	The proceeds of the Performance Security (or Guarantee) shall be payable to the Procuring Agency as compensation for any loss resulting from the Supplier's failure to complete its obligations under the Contract.
		12.2	The Performance Guarantee shall be in one of the following forms:

			a)	A bank guarantee, an irrevocable letter of credit issued by a reputable bank, or in the form provided in the Bidding Documents or another form acceptable to the Procuring Agency; or
			b)	A cashier's or certified check.
		12.3	The performance guarantee will be discharged by the Procuring Agency and returned to the Supplier not later than thirty (30) days following the date of completion of the Supplier's performance obligations under the Contract, including any warranty obligations, unless otherwise specified in **SCC**.	
13.	**Taxes and Duties**	13.1	A foreign Supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside Pakistan.	
		13.2	If any tax exemptions, reductions, allowances or privileges may be available to the Supplier in Pakistan the Procuring Agency shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent.	
		13.3	A local Supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until the supply of the TBMLsystem to the Procuring Agency.	
14.	**Copy Rights**	14.1	The Intellectual Property Rights in all Standard Software and Standard Materials shall remain vested in the owner of such rights.	
		14.2	The Procuring agency agrees to restrict use, copying, or duplication of the Standard Software and Standard Materials in accordance with GCC Clause 16, except those additional copies of Standard Materials may be made by the Procuring agency for use within the	
		14.3	The Procuring agency's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except in accordance with the relevant license agreement or as may be otherwise specified in the **SCC**	

		14.5	As applicable, the Procuring agency's and Supplier's rights and obligations with respect to Custom Software or elements of the Custom Software, including any license agreements, and with respect to Custom Materials or elements of the Custom Materials, are specified in the **SCC**. Subject to the SCC, the Intellectual Property Rights in all Custom Software and Custom Materials specified in the Contract Agreement (if any) shall, at the date of this Contract or on creation of the rights (if later than the date of this Contract), vest in the Procuring agency. The Supplier shall do and execute or arrange for the doing and executing of each necessary act, document, and thing that the Procuring agency may consider necessary or desirable to perfect the right, title, and interest of the Procuring agency in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of a moral right in such an item does not assert it, and the Supplier shall, if requested to do so by the Procuring agency, and where permitted by applicable law, ensure that the holder of such a moral right waives it.
		14.6	The parties shall enter into such (if any) escrow arrangements in relation to the Source Code to some or all of the Software as are **specified in the SCC** and in **accordance with the SCC**
15.	**Software License Agreements**	15.1	Except to the extent that the Intellectual Property Rights in the Software vest in the Procuring agency, the Supplier hereby grants to the Procuring agency license to access and use the Software, including all inventions, designs, and marks embodied in the Software. Such license to access and use the Software shall: a) be: i. nonexclusive;
			ii. fully paid up and irrevocable (except that it shall terminate if the Contract terminates under GCC Clauses 41; iii. valid throughout the territory of the Procuring agency's Country (or such other territory as specified in the SCC); and iv. subject to additional restrictions (if any) as specified in the SCC.

			b) permit the Software to be: i. used or copied for use on or with the computer(s) for which it was acquired (if specified in the Technical Requirements and/or the Supplier's bid), plus a backup computer(s) of the same or similar capacity, if the primary is(are) inoperative, and during a reasonable transitional period when use is being transferred between primary and backup; ii. as specified in the SCC, used or copied for use on or transferred to a replacement computer(s), (and use on the original and replacement computer(s) may be simultaneous during a reasonable transitional period) provided that, if the Technical Requirements and/or the Supplier's bid specifies a class of computer to which the license is restricted and unless the Supplier agrees otherwise in writing, the replacement computer(s) is(are) within that class; iii. if the nature of the System is such as to permit such access, accessed from other computers connected to the primary and/or backup computer(s) by means of a local or wide-area network or similar arrangement, and used on or copied for use on those other computers to the extent necessary to that access;
			iv. reproduced for safekeeping or backup purposes; v. customized, adapted, or combined with other computer software for use by the Procuring agency, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to same restrictions as are set forth in this Contract; vi. as specified in the SCC, disclosed to, and reproduced for use by, support service suppliers and their subcontractors, (and the Procuring agency may sublicense such persons to use and copy for use the Software) to the extent reasonably necessary to the performance of their support service contracts, subject to the same restrictions as are set forth in this Contract; and
			(vii) disclosed to, and reproduced for use by, the Procuring agency and by such other persons as are specified in the SCC (and the Procuring agency may sublicense such persons to use and copy for use the Software), subject to the same restrictions as are set forth in this Contract.

		15.2	The Standard Software may be subject to audit by the Supplier, in accordance with the terms **specified in the SCC**, to verify compliance with the above license agreements.
16.	**Confidential Information**	16.1	Except if otherwise specified in the SCC, the "Receiving Party" (either the Procuring agency or the Supplier) shall keep confidential and shall not, without the written consent of the other party to this Contract ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information") connected with this Contract, and furnished directly or indirectly by the Disclosing Party prior to or during performance, or following termination, of this Contract.
		16.2	For the purposes of GCC Clause 16.1, the Supplier is also deemed to be the Receiving Party of Confidential Information generated by the Supplier itself in the course of the performance of its obligations under the Contract and relating to the businesses, finances, suppliers, employees, or other contacts of the Procuring agency or the Procuring agency's use of the System.
		16.3	Notwithstanding GCC Clauses 16.1 and 16.2: a) the Supplier may furnish to its Subcontractor Confidential Information of the Procuring agency to the extent reasonably required for the Subcontractor to perform its work under the Contract; and b) the Procuring agency may furnish Confidential Information of the Supplier: (i) to its support service suppliers and their subcontractors to the extent reasonably required for them to perform their work under their support service contracts; and (ii) to its affiliates and subsidiaries, in which event the Receiving Party shall ensure that the person to whom it furnishes Confidential Information of the Disclosing Party is aware of and abides by the Receiving Party's obligations under this GCC Clause 16 as if that person were party to the Contract in place of the Receiving Party.

		16.4	The Procuring agency shall not, without the Supplier's prior written consent, use any Confidential Information received from the Supplier for any purpose other than the operation, maintenance and further development of the System. Similarly, the Supplier shall not, without the Procuring agency's prior written consent, use any Confidential Information received from the Procuring agency for any purpose other than those that are required for the performance of the Contract.
		16.5	The obligation of a party under GCC Clauses 16.1 through 16.4 above, however, shall not apply to that information which: a) now or hereafter enters the public domain through no fault of the Receiving Party; b) can be proven to have been possessed by the Receiving Party at the time of disclosure and that was not previously obtained, directly or indirectly, from the Disclosing Party; c) otherwise lawfully becomes available to the Receiving Party from a third party that has no obligation of confidentiality.
		16.6	The above provisions of this GCC Clause 16 shall not in any way modify any undertaking of confidentiality given by either of the parties to this Contract prior to the date of the Contract in respect of the System or any part thereof.
		16.7	The provisions of this GCC Clause 16 shall survive the termination, for whatever reason, of the Contract for three (3) years or such longer period as may be specified in the SCC.
17.	**Project Plan**	17.1	In close cooperation with the Procuring agency and based on the Preliminary Project Plan included in the Supplier's bid, the Supplier shall develop a Project Plan encompassing the activities specified in the Contract. The contents of the Project Plan shall be as specified in the SCC and/or Technical Requirements.
		17.2	The Supplier shall formally present to the Procuring agency the Project Plan in accordance with the procedure specified in the SCC
		17.3	If required, the impact on the Implementation Schedule of modifications agreed during finalization of the Agreed and Finalized Project Plan shall be incorporated in the Contract by amendment, in accordance with GCC Clauses 35.

		17.4	The Supplier shall undertake to supply, install, test, and commission the System in accordance with the Agreed and Finalized Project Plan and the Contract
		17.5	The Progress and other reports **specified in the SCC** shall be prepared by the Supplier and submitted to the Procuring agency in the format and frequency specified in the Technical Requirements.
18.	**Sub-contracting**	18.1	List of Approved Subcontractors to the Contract Agreement specifies critical items of supply or services and a list of Subcontractors for each item that are considered acceptable by the Procuring agency. If no Subcontractors are listed for an item, the Supplier shall prepare a list of Subcontractors it considers qualified and wishes to be added to the list for such items. The Supplier may from time to time propose additions to or deletions from any such list. The Supplier shall submit any such list or any modification to the list to the Procuring agency for its approval in sufficient time so as not to impede the progress of work on the System. The Procuring agency shall not withhold such approval unreasonably. Such approval by the Procuring agency of a Subcontractor(s) shall not relieve the Supplier from any of its obligations, duties, or responsibilities under the Contract
		18.2	The Supplier may, at its discretion, select and employ Subcontractors for such critical items from those Subcontractors listed pursuant to GCC Clause 18.1. If the Supplier wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek the Procuring agency's prior approval under GCC Clause 18.3.

		18.3	For items for which pre-approved Subcontractor lists have not been specified in Appendix to the Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided: (i) the Supplier notifies the Procuring agency in writing at least twenty-eight (28) days prior to the proposed mobilization date for such Subcontractor; and (ii) by the end of this period either the Procuring agency has granted its approval in writing or fails to respond. The Supplier shall not engage any Subcontractor to which the Procuring agency has objected in writing prior to the end of the notice period. The absence of a written objection by the Procuring agency during the above specified period shall constitute formal acceptance of the proposed Subcontractor. Except to the extent that it permits the deemed approval of the Procuring agency of Subcontractors not listed in the Contract Agreement, nothing in this Clause, however, shall limit the rights and obligations of either the Procuring agency or Supplier as they are specified in GCC Clauses 18.1 and 18.2, in the SCC, or in Appendix of the Contract Agreement.
19.	**Procurement and Delivery**	19.1	Subject to related Procuring agency's responsibilities pursuant to GCC Clause 9, the Supplier shall manufacture or procure and transport all the Information Technologies, Materials, and other Goods in an expeditious and orderly manner to the Project Site
		19.2	Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier in accordance with the Technical Requirements
		19.3	Early or partial deliveries require the explicit written consent of the Procuring agency, which consent shall not be unreasonably withheld.
20.	**Transportation**	20.1	The Supplier shall provide such packing of the Goods as is required to prevent their damage or deterioration during shipment. The packing, marking, and documentation within and outside the packages shall comply strictly with the Procuring agency's instructions to the Supplier.
		20.2	The Supplier will bear responsibility for and cost of transport to the Project Sites in accordance with the terms and conditions used in the specification of prices in the Price Schedules, including the terms and conditions of the associated Incoterms.
		20.3	Unless otherwise specified in the SCC, the Supplier shall be free to use transportation through carriers registered in any eligible country and to obtain insurance from any eligible source country.

21.	**Documents**	21.1	Unless otherwise specified in the SCC, the Supplier will provide the Procuring agency with shipping and other documents, as specified below; i. For Goods supplied from outside the Procuring agency's Country: Upon shipment, the Supplier shall notify the Procuring agency and the insurance company contracted by the Supplier to provide cargo insurance by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Procuring agency by mail or courier, as appropriate, with a copy to the cargo insurance company: a) two copies of the Supplier's invoice showing the description of the Goods, quantity, unit price, and total amount; b) usual transportation documents; c) insurance certificate; d) certificate(s) of origin; and e) estimated time and point of arrival in the Procuring agency's Country and at the site. ii. For Goods supplied locally (i.e., from within the Procuring agency's country): Upon shipment, the Supplier shall notify the Procuring agency by telex, cable, facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the Procuring agency by mail or courier, as appropriate: a) two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount; b) delivery note, railway receipt, or truck receipt; c) certificate of insurance; d) certificate(s) of origin; and e) estimated time of arrival at the site.

			iii. Customs Clearance a) The Procuring agency will bear responsibility for, and cost of, customs clearance into the Procuring agency's country in accordance the particular Incoterm(s) used for Goods supplied from outside the Procuring agency's country in the Price Schedules referred to by Article 2 of the Contract Agreement. b) At the request of the Procuring agency, the Supplier will make available a representative or agent during the process of customs clearance in the Procuring agency's country for goods supplied from outside the Procuring agency's country. In the event of delays in customs clearance that are not the fault of the Supplier: c) the Supplier shall be entitled to an extension in the Time for Achieving Operational Acceptance, pursuant to GCC Clause 26; the Contract Price shall be adjusted to compensate the Supplier for any additional storage charges that the Supplier may incur as a result of the delay.
22.	**Product Upgrades**	22.1	At any point during performance of the Contract, should technological advances be introduced by the Supplier for Information Technologies originally offered by the Supplier in its bid and still to be delivered, the Supplier shall be obligated to offer to the Procuring agency the latest versions of the available Information Technologies having equal or better performance or functionality at the same or lesser unit prices.
		22.2	At any point during performance of the Contract, for Information Technologies still to be delivered, the Supplier will also pass on to the Procuring agency any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in the Procuring agency's Country.
			During performance of the Contract, the Supplier shall offer to the Procuring agency all new versions, releases, and updates of Standard Software, as well as related documentation and technical support services, within thirty (30) days of their availability from the Supplier to other clients of the Supplier in the Procuring agency's Country, and no later than twelve (12) months after they are released in the country of origin. In no case will the prices for these Software exceed those quoted by the Supplier in the Recurrent Costs tables in its bid.

23.	**Inspections and Test**	23.1	The Procuring Agency or its representative shall have the right to inspect and /or to test the components of the system to confirm their conformity to the Contract specifications at no extra cost to the Procuring Agency. **SCC** and the Technical Specifications shall specify what inspections and tests the Procuring Agency shall notify the Supplier in writing or in electronic forms that provide record of the content of communication, in a timely manner, of the identity of any representatives retained for these purposes.
		23.2	The inspections and tests may be conducted on the premises of the Supplier or its subcontractor(s), at point of delivery, and/or at the Goods' final destination. If conducted on the premises of the Supplier or its subcontractor(s), all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the Procuring Agency.
		23.3	Should any inspected or tested component fail to conform to the Specifications, the Procuring Agency may reject the component, and the Supplier shall replace the rejected component to meet specification requirements free of cost to the Procuring Agency.
		23.4	The Procuring Agency's right to inspect, test and, where necessary, reject component after' arrival in the Procuring Agency's country shall in no way be limited or eared by reason of the component having previously been inspected, tested, and passed by the Procuring Agency or its representative prior to the shipment from the country of origin.
		23.5	The Procuring Agency may require the Supplier to carry out any inspection and/or test not specified in the Contract, provided that the Supplier's reasonable costs and expenses incurred in the carrying out of such inspection and/or test shall be added to the Contract Price. Further, if such inspection and/or test impedes the progress of work on the System and/or the Supplier's performance of its other obligations under the Contract, due allowance will be made in respect of the Time for Achieving Operational Acceptance and the other obligations so affected
		23.6	If any dispute shall arise between the parties in connection with or caused by an inspection and/or with regard to any component to be incorporated in the System that cannot be settled amicably between the parties within a reasonable period of time, either party may invoke the process, starting with referral of the matter to the Adjudicator in case an Adjudicator is included and named in the Contract Agreement.

24.	**Installation of the System**	24.1	As soon as the System, or any Subsystem, has, in the opinion of the Supplier, been delivered, pre-commissioned, and made ready for Commissioning and Operational Acceptance Testing in accordance with the Technical Requirements, the SCC and the Agreed and Finalized Project Plan, the Supplier shall so notify the Procuring agency in writing
		24.2	The Project Manager shall, within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 24.1, either issue an Installation Certificate in the form specified in the Sample Forms Section in the Bidding Documents, stating that the System, or major component or Subsystem (if Acceptance by major component or Subsystem is specified pursuant to the SCC for GCC Clause 26.1), has achieved Installation by the date of the Supplier's notice under GCC Clause 24.1, or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability or integration of the various components and/or Subsystems making up the System. The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies that the Project Manager has notified the Supplier of. The Supplier shall then promptly carry out retesting of the System or Subsystem and, when in the Supplier's opinion the System or Subsystem is ready for Commissioning and Operational Acceptance Testing, notify the Procuring agency in writing, in accordance with GCC Clause 24.1. The procedure set out in this GCC Clause 24.2 shall be repeated, as necessary, until an Installation Certificate is issued.
		24.3	If the Project Manager fails to issue the Installation Certificate and fails to inform the Supplier of any defects and/or deficiencies within fourteen (14) days after receipt of the Supplier's notice under GCC Clause 24.1, or if the Procuring agency puts the System or a Subsystem into production operation, then the System (or Subsystem) shall be deemed to have achieved successful Installation as of the date of the Supplier's notice or repeated notice, or when the Procuring agency put the System into production operation, as the case may be.
25.	**Commissioning**	25.1	Commissioning of the System (or Subsystem if specified pursuant to the SCC for GCC Clause 26.1) shall be commenced by the Supplier: immediately after the Installation Certificate is issued by the Project Manager, pursuant to GCC Clause 24.2; or as otherwise specified in the Technical Requirement or the Agreed and Finalized Project Plan; or immediately after Installation is deemed to have occurred, under GCC Clause 24.3.

		25.2	The Procuring agency shall supply the operating and technical personnel and all materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning. Production use of the System or Subsystem(s) shall not commence prior to the start of formal Operational Acceptance Testing
26.	**Operational Acceptance Tests**	26.1	The Operational Acceptance Tests (and repeats of such tests) shall be the primary responsibility of the Procuring agency (in accordance with GCC Clause 9.9), but shall be conducted with the full cooperation of the Supplier during Commissioning of the System (or major components or Subsystem[s] if specified in the SCC and supported by the Technical Requirements), to ascertain whether the System (or major component or Subsystem[s]) conforms to the Technical Requirements and meets the standard of performance quoted in the Supplier's bid, including, but not restricted to, the functional and technical performance requirements. The Operational Acceptance Tests during Commissioning will be conducted as specified in the SCC, the Technical Requirements and/or the Agreed and Finalized Project Plan. At the Procuring agency's discretion, Operational Acceptance Tests may also be performed on replacement Goods, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System.
		26.2	If for reasons attributable to the Procuring agency, the Operational Acceptance Test of the System (or Subsystem[s] or major components, pursuant to the SCC for GCC Clause 26.1) cannot be successfully completed within the period specified in the SCC, from the date of Installation or any other period agreed upon in writing by the Procuring agency and the Supplier, the Supplier shall be deemed to have fulfilled its obligations with respect to the technical and functional aspects of the Technical Specifications, SCC and/or the Agreed and Finalized Project Plan.

27.	**Operational Acceptance**	27.1	Subject to GCC Clause 27.4 (Partial Acceptance) below, Operational Acceptance shall occur in respect of the System, when a) the Operational Acceptance Tests, as specified in the Technical Requirements, and/or SCC and/or the Agreed and Finalized Project Plan have been successfully completed; or b) the Operational Acceptance Tests have not been successfully completed or have not been carried out for reasons that are attributable to the Procuring agency within the period from the date of Installation or any other agreed-upon period as specified in GCC Clause 27.2.2 above; or c) the Procuring agency has put the System into production or use for sixty (60) consecutive days. If the System is put into production or use in this manner, the Supplier shall notify the Procuring agency and document such use
		27.2	At any time after any of the events set out in GCC Clause 27.1 have occurred, the Supplier may give a notice to the Project Manager requesting the issue of an Operational Acceptance Certificate.
		27.3	After consultation with the Procuring agency, and within fourteen (14) days after receipt of the Supplier's notice, the Project Manager shall: a) issue an Operational Acceptance Certificate; or b) notify the Supplier in writing of any defect or deficiencies or other reason for the failure of the Operational Acceptance Tests; or c) issue the Operational Acceptance Certificate, if the situation covered by GCC Clause 27.1 (b) arises.

		27.4	The Supplier shall use all reasonable endeavors to promptly remedy any defect and/or deficiencies and/or other reasons for the failure of the Operational Acceptance Test that the Project Manager has notified the Supplier of. Once such remedies have been made by the Supplier, the Supplier shall notify the Procuring agency, and the Procuring agency, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify the Procuring agency of its request for Operational Acceptance Certification, in accordance with GCC Clause 27.3. The Procuring agency shall then issue to the Supplier the Operational Acceptance Certification in accordance with GCC Clause 27.3 (a), or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this GCC Clause 27.4 shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.
		27.5	If the System or Subsystem fails to pass the Operational Acceptance Test(s) in accordance with GCC Clause 26.1, then either: a) the Procuring agency may consider terminating the Contract, pursuant to GCC Clause 41; or b) if the failure to achieve Operational Acceptance within the specified time period is a result of the failure of the Procuring agency to fulfill its obligations under the Contract, then the Supplier shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract.
		27.6	If within fourteen (14) days after receipt of the Supplier's notice the Project Manager fails to issue the Operational Acceptance Certificate or fails to inform the Supplier in writing of the justifiable reasons why the Project Manager has not issued the Operational Acceptance Certificate, the System or Subsystem shall be deemed to have been accepted as of the date of the Supplier's said notice

28.	**Partial Acceptance**	28.1	If so specified in the SCC for GCC Clause 26.1, Installation and Commissioning shall be carried out individually for each identified major component or Subsystem(s) of the System. In this event, the provisions in the Contract relating to Installation and Commissioning, including the Operational Acceptance Test, shall apply to each such major component or Subsystem individually, and Operational Acceptance Certificate(s) shall be issued accordingly for each such major component or Subsystem of the System, subject to the limitations contained in GCC Clause 28.2
		28.2	The issuance of Operational Acceptance Certificates for individual major components or Subsystems pursuant to GCC Clause 28.1 shall not relieve the Supplier of its obligation to obtain an Operational Acceptance Certificate for the System as an integrated whole (if so specified in the SCC for GCC 27.1) once all major components and Subsystems have been supplied, installed, tested, and commissioned
		28.3	In the case of minor components for the System that by their nature do not require Commissioning or an Operational Acceptance Test (e.g., minor fittings, furnishings or site works, etc.), the Project Manager shall issue an Operational Acceptance Certificate within fourteen (14) days after the fittings and/or furnishings have been delivered and/or installed or the site works have been completed. The Supplier shall, however, use all reasonable endeavors to promptly remedy any defects or deficiencies in such minor components detected by the Procuring agency or Supplier.
29.	**Warranty/ Defect Liability Period**	29.1	The Supplier warrants that the system, including all Information Technologies, Materials and other goods supplied and services provided under the Contract are new, unused, of the most recent or current models and that they incorporate all recent improvements in design and materials unless provided otherwise in the Contract. The Supplier further warrants that all Goods supplied and services provided under this Contract shall have no defect, arising from design, materials, or workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements (except when the design and/or material is required by the Procuring Agency, specifications) or from any act or omission of the Supplier, that may develop under normal use of the supplied TBML System in the conditions prevailing in Pakistan. Exceptions and/or limitations, if any, to this warranty with respect to Software (or categories of Software), shall be as specified in the SCC. Commercial warranty provisions of products supplied under the Contract shall apply to the extent that they do not conflict with the provisions of this Contract.

		29.2	This warranty Period shall commence from the date of Operational Acceptance of the System (or of any major component or Subsystem for which separate Operational Acceptance is provided for in the Contract) and shall remain valid for a period specified in the **SCC**.
		29.3	The Procuring Agency shall promptly notify the Supplier in writing or in electronic forms that provide record of the content of communication of any claims arising under this warranty.
		29.4	Upon receipt of such notice, the Supplier shall promptly or within the period specified in the SCC, in consultation and agreement with the Procuring agency regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good (as the Supplier shall, at its discretion, determine) such defect as well as any damage to the System caused by such defect. Any defective Information Technologies or other Goods that have been replaced by the Supplier shall remain the property of the Supplier
		29.5	If the Supplier, having been notified, fails to remedy the defect(s) within the period specified in **SCC**, the Procuring Agency may proceed to take such remedial action as may be necessary, at the Supplier's risk and expense and without prejudice to any other rights which the Procuring Agency may have against the Supplier under the Contract.
30.	**Intellectual Property Rights Indemnity**	30.1	The Supplier shall indemnify and hold harmless the Procuring agency and its employees and officers from and against any and all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that the Procuring agency or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights by reason of: a) installation of the System by the Supplier or the use of the System, including the Materials, in the country where the site is located; b) copying of the Software and Materials provided the Supplier in accordance with the Agreement; and c) sale of the products produced by the System in any country, except to the extent that such losses, liabilities, and costs arise as a result of the Procuring agency's breach of GCC Clause 30.2.

		30.2	Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose indicated by or to be reasonably inferred from the Contract, any infringement resulting from the use of the System, or any products of the System produced thereby in association or combination with any other goods or services not supplied by the Supplier, where the infringement arises because of such association or combination and not because of use of the System in its own right.
		30.3	Such indemnities shall also not apply if any claim of infringement: a) is asserted by a parent, subsidiary, or affiliate of the Procuring agency's organization; b) is a direct result of a design mandated by the Procuring agency's Technical Requirements and the possibility of such infringement was duly noted in the Supplier's Bid; or c) results from the alteration of the System, including the Materials, by the Procuring agency or any persons other than the Supplier or a person authorized by the Supplier
31.	**Insurance**	31.1	The TBML System supplied/provided under the Contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage, and delivery in the manner specified in the SCC.
32.	**Limitation of Liability**	32.1	Provided the following does not exclude or limit any liabilities of either party in ways not permitted by applicable law: a) the Supplier shall not be liable to the Procuring agency, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the Supplier to pay liquidated damages to the Procuring agency; and b) the aggregate liability of the Supplier to the Procuring agency, whether under the Contract, in tort or otherwise, shall not exceed the total Contract Price, provided that this limitation shall not apply to any obligation of the Supplier to indemnify the Procuring agency with respect to intellectual property rights infringement
33.	**Related Services**	33.1	The Supplier may be required to provide any or all of the following services, including additional services, if any, specified in **SCC**:

			a)	Performance or supervision of on-site assembly, Installation Commissioning and/or start-up of the supplied Goods;
			b)	Furnishing of tools required for assembly and/or maintenance of the supplied Goods;
			c)	Furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied Goods;
			d)	Performance or supervision or maintenance and/or repair of the supplied Goods, for a period of time agreed by the parties, provided that this service shall not relieve the Supplier of any warranty obligations under this Contract; and
			e)	Training of the Procuring Agency's personnel, at the Supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the Goods supplied and Services Provided.
		33.2	Prices charged by the Supplier for related services, if not included in the Contract, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.	
34.	**Change Orders**	34.1	The Procuring Agency may at any time, by a written order given to the Supplier, make changes within the general scope of the Contract in any one or more of the following:	
			a)	Drawings, designs, or specifications;
			b)	The method of shipment or packing;
			c)	The place of delivery; and/or
			d)	The Services to be provided by the Supplier.
		34.2	If any such change causes an increase or decrease in the cost of, or the time required for, the Supplier's performance of any provisions under the Contract an equitable adjustment shall be made in the Contract Price or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the Supplier for adjustment under this clause must be asserted within thirty (30) days from the date of the Supplier's receipt of the Procuring Agency change order.	
		34.3	Prices to be charged by the supplier for any related services that might be needed but which were not included in the Contract shall be agreed upon in advance by the Parties and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.	
35.	**Contract Amendments**	35.1	Subject to **GCC Clause 34**, no variation in or modification of the terms of the Contract shall be made except by written amendment signed by the parties.	

36.	**Assignment**	36.1	Neither the Procuring Agency nor the Supplier shall assign, in whole or in part, obligations under this Contract, except with the prior written consent of the other party.
37.	**Sub-contracts**	37.1	The Supplier shall consult the Procuring Agency in the event of subcontracting under this contract if not already specified in the Bid. Subcontracting shall not alter the Supplier's obligations.
38.	**Delays in the Supplier's Performance**	38.1	Delivery of the Goods and performance of Services making TBMLsystem shall be made by the Supplier in accordance with the time schedule prescribed by the Procuring Agency in the Schedule of Requirements.
		38.2	If at any time during performance of the Contract, the Supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the Goods and performance of Services, the Supplier shall promptly notify the Procuring Agency in writing or in electronic forms that provide record of the content of communication of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the Supplier's notice, the Procuring Agency shall evaluate the situation and may at its discretion extend the Supplier's time for performance, with or without liquidated damages, in which case the extension shall be ratified by the parties by amendment of Contract.
		38.3	Except as provided under GCC Clause 41, a delay by the Supplier in the performance of its delivery obligations shall render the Supplier liable to the imposition of liquidated damages pursuant to GCC Clause 39, unless an extension of time is agreed upon pursuant to GCC Clause 38.2 without the application of liquidated damages.
39.	**Liquidated Damages**	39.1	Subject to GCC Clause 41, if the Supplier fails to deliver any or all of the Goods or to perform the Services within the period(s) specified in the Contract, the Procuring Agency shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum equivalent to the percentage specified in SCC of the delivered price of the delayed Goods or unperformed Services for each week or part thereof of delay until actual delivery or performance, up to a maximum deduction of the performance security (or guarantee) specified in SCC. Once the said maximum is reached, the Procuring Agency may consider termination of the Contract pursuant to GCC Clause 40.
40.	**Termination for Default**	40.1	The Procuring Agency or the Supplier, without prejudice to any other remedy for breach of Contract, by written notice of default sent to the concerned party may terminate the Contract if the other party causes a
		40.2	Fundamental breaches of Contract shall include, but shall not be limited to the following:

			a)	the Supplier fails to deliver any or all of the Goods within the period(s) specified in the Contract, or within any extension thereof granted by the Procuring Agency or
			b)	the Supplier fails to perform any other obligation(s) under the Contract;
			c)	Supplier's failure to submit performance security (or guarantee) within the time stipulated in the **SCC**;
			d)	the supplier has abandoned or repudiated the contract.
			e)	the Procuring Agency or the Supplier is declared bankrupt or goes into liquidation other than for a reconstruction or amalgamation;
			f)	a payment is not paid by the Procuring Agency to the Supplier after 84 days from the due date for payment;
			g)	the Procuring Agency gives Notice that goods delivered with a defect is a fundamental breach of Contract and the Supplier fails to correct it within a reasonable period of time determined by the Procuring Agency; and
			h)	if the Procuring Agency determines, based on the reasonable evidence, that the Supplier has engaged in corrupt, coercive, collusive, obstructive or fraudulent practices, in competing for or in executing the Contract.
		40.3	or the purpose of this clause:	
			"**Corrupt and Fraudulent Practice**" means the practices as described in Rule-2 (1) (f) of Public Procurement Rules-2004.	
		40.4	In the event the Procuring Agency terminates the Contract in whole or in part, pursuant to **GCC Clause 26.1**, the Procuring Agency may procure, upon such terms and in such manner as it deems appropriate, Goods or Services similar to those undelivered, and the Supplier shall be liable to the Procuring Agency for any excess costs for such similar Goods or Services. However, the Supplier shall continue performance of the Contract to the extent not terminated.	

41.	**Termination for Force Majeure**	41.1	Notwithstanding the provisions of **GCC Clauses 38, 39,** and 40, neither Party shall have any liability or be deemed to be in breach of the Contract for any delay nor is other failure in performance of its obligations under the Contract, if such delay or failure is a result of an event of Force Majeure. For purpose of this clause, ''Force Majeure'' means an event which is beyond the reasonable control of a Party, is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of a Party, and which makes a Party's performance of its obligations hereunder impossible or so impractical as reasonably to be considered impossible in the circumstances, and includes, but is not limited to, war, riots, civil disorder, earthquake, fire, explosion, storm, flood, epidemics, or other adverse weather conditions, strikes, lockouts or other industrial action (except where such strikes, lockouts or other industrial action are within the power of the Party invoking Force Majeure to prevent
		41.2	If a Party (hereinafter referred to as "the Affected Party") is or will be prevented from performing its substantial obligation under the contract by Force Majeure, it shall give a Notice to the other Party giving full particulars of the event and circumstance of Force Majeure in writing or in electronic forms that provide record of the content of communication of such condition and the cause thereof. Unless otherwise directed by the Procuring Agency in writing or in electronic forms that provide record of the content of communication, the Supplier shall continue to perform its obligations under the Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.
42.	**Termination for Insolvency**	42.1	The Procuring Agency may at any time terminate the Contract by giving written notice to the Supplier if the Supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Procuring Agency.
43.	**Termination for Convenience**	43.1	The Procuring Agency, by written notice sent to the Supplier, may terminate the contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Procuring Agency's convenience, the Contract is terminated, and the date upon which such termination becomes effective.

		43.2	The Systems that are complete and ready for shipment within thirty (30) days after the Supplier's receipt of notice of termination shall be accepted by the Procuring Agency at the Contract terms and price. For the remaining system, the Procuring Agency may elect:
			a) To have any portion completed and delivered at the Contract terms and prices; and / or
			b) To cancel the remainder and pay to the Supplier an agreed amount for partially completed Goods and Services and for materials and parts previously procured by the Supplier.
44.	**Transfer of Ownership**	44.1	With the exception of Software and Materials, the ownership of the Information Technologies and other Goods shall be transferred to the Procuring agency at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement.
		44.2	Ownership and the terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC Clause 14 (Copyright) and any elaboration in the Technical Requirements
		44.3	Ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract shall remain with the Supplier or its Subcontractors.
45.	**Disputes Resolution**	45.1	In the event of any dispute arising out of this contract, either party shall issue a notice of dispute to settle the dispute amicably. The parties hereto shall, within twenty-eight (28) days from the notice date, use their best efforts to settle the dispute amicably through mutual consultations and negotiation. Any unsolved dispute may be referred by either party to an arbitrator that shall be appointed by mutual consent of the both parties.
		45.2	After the dispute has been referred to the arbitrator, within 30 days, or within such other period as may be proposed by the Parties, the Arbitrator shall give its decision. The rendered decision shall be binding to the Parties.
46.	**Procedure for Disputes Resolution**	46.1	The arbitration shall be conducted in accordance with the arbitration procedure published by the Institution named and, in the place, shown in the **SCC**.
		46.2	The rate of the Arbitrator's fee and administrative costs of arbitration shall be borne equally by the Parties. The rates and costs shall be in accordance with the rules of the Appointing Authority. In conducting arbitration to its finality each party shall bear its incurred costs and expenses.
		46.3	The arbitration shall be conducted in accordance with the arbitration procedure published by the institution named and, in the place, shown in the **SCC**.

47.	**Replacement of Arbitrator**	47.1	Should the Arbitrator resign or die, or should the Procuring Agency and the Supplier agree that the Arbitrator is not functioning in accordance with the provisions of the contract, a new Arbitrator shall be appointed by mutual consent of the both parties.
48.	**Notices**	48.1	Any notice given by one party to the other pursuant to this Contract shall be sent to the other party in writing or in electronic forms that provide record of the content of communication and confirmed in writing or in electronic forms that provide record of the content of communication to the other party's address specified in **SCC**.
		48.2	A notice shall be effective when delivered or on the notice's effective date, whichever is later.

SECTION VIII: SPECIAL CONDITIONS OF THE CONTRACT (SCC)

Special Conditions of Contract (SCC)

The following Special Conditions of Contract (SCC) shall supplement the GCC. Whenever there is a conflict, the provisions herein shall prevail over those in the GCC. The corresponding clause number of the GCC is indicated in parentheses.

SCC Clause Number	GCC Clause Number	Amendments of, and Supplements to, Clauses in the GCC
Definitions (GCC 1)		
1.	1.1	The Procuring Agency is: National Bank of Pakistan NBP Head Office Building I.I. Chundrigar Road , Karachi, Pakistan
2.	1.1(j)	The Supplier is:
3.	1.1(q)	The title of the subject procurement or The Project is: **TRADE BASED MONEY LAUNDERING SYSTEM**
Governing Language (GCC 4)		
4.	4.1	The Governing Language shall be: English
Applicable Law (GCC 5)		
5.	5.1	The Applicable Law shall be: Laws of PAKISTAN
	5.2	The Contract shall be effective from the date……
Country of Origin (GCC 6)		
6.	6.1	Country of Origin is Pakistan
Scope of the System (GCC 7)		
7.	7.1	Please refer to the Technical Specification in section V
Supplier Responsibilities (GCC 8)		

8.	8.1	The Supplier shall have the following additional responsibilities: **Please refer to section V**
Procuring Agency's Responsibilities (GCC 9)		
9.	9.1	The Procuring agency shall have the following additional responsibilities: **Please refer to section V**
Price (GCC 10)		
10.	10.1	Prices shall be adjusted in accordance with provisions in the Attachment to SCC. **Please refer to section V**
Payment (GCC 11)		
11.	11.1	The method and conditions of payment to be made to the Supplier under this Contract shall be as follows: **Please refer to the payment plan in section V**
12.	11.2	**Payment for Goods and Services supplied from within Pakistan:** **Please refer to the payment plan in section V**
13.	11.3	Rate to be used for paying the Supplier's interest on the late payment made by Procuring Agency shall be **Please refer to section V**
Performance Guarantee (GCC 12)		
14.	12.1	The amount of performance guarantee, as a percentage of the Contract Price, shall be: **Please refer to the payment plan in section V**
15.	12.4	After delivery and acceptance of the TBML System, 10 percent of the Performance Guarantee shall be withheld to cover the Supplier's warranty obligations in accordance with **GCC Clause 29.**
Taxes and Duties (GCC 13)		
16.	13.	***"There are no Special Conditions of Contract applicable to GCC Clause 13"***
Copy Rights (GCC 14)		

17.	14.3	The Procuring agency may assign, license, or otherwise voluntarily transfer its contractual rights to use the Standard Software or elements of the Standard Software, without the Supplier's prior written consent, under the following circumstances: none
18.	14.4	The Procuring agencies and Supplier's rights and obligations with respect to Custom Software or elements of the Custom Software are as follows *not applicable*
		The Procuring agencies and Supplier's rights and obligations with respect to Custom Materials or elements of the Custom Materials are as follows Not applicable
19.	14.5	Maximum number of days during which a separate escrow contract must be agreed upon with a reputable escrow agent and any specific rights and obligations that the Procuring agency wishes to establish in advance.
Software License Validity (GCC 15)		
20.	15.1 (a)(iii)	The Standard Software license shall be valid *for NBP use.*
21.	15.1 (a)(iv)	Use of the software shall be subject to the following additional restrictions *None*
22.	15.1(b)(ii)	The Software license shall permit the Software to be used or copied for use or transferred to a replacement computer ***"provided the replacement computer falls within approximately the same class of machine and maintains approximately the same number of users, if a multi-user machine;"***
23.	15.1(b)(vii)	The Software license shall permit the Software to be disclosed to and reproduced for use (including a valid sublicense) by ***"support service suppliers or their subcontractors, exclusively for such suppliers or subcontractors in the performance of their support service contracts;"***
Confidential Information (GCC 16)		
24.	16.1	*State:* ***"There are no modifications to the confidentiality terms expressed in GCC Clause 16.1;"***
25.	16.7	*The provisions of this GCC Clause 16 shall survive the termination, for whatever reason, of the Contract for* as mentioned in GCC

Project Plan (GCC 17)		
26.	17.1	***"There are no Special Conditions of Contract applicable to GCC Clause please refer section V***
27.	17.2	***"There are no Special Conditions of Contract applicable to GCC Clause*** Please refer section V
28.	17.5	***"There are no Special Conditions of Contract applicable to GCC Clause,*** Please refer section V
Sub-Contracting (GCC 18)		
29.	18.1	***"There are no Special Conditions of Contract applicable to GCC Clause 18."***
Transportation (GCC 19)		
30.	19.1	The Supplier *shall* be free to use transportation through carriers registered in any eligible country and *shall* obtain insurance from any eligible source country.
Documents (GCC 21)		
31.	21.1	The Supplier shall provide to the Procuring agency documents *[state* ***"as specified in the GCC,"***
Products Upgrade (GCC 22)		
32.	22.1	The Supplier shall provide the Procuring agency: ***"with all new versions, releases, and updates to all Standard Software during the Warranty Period, for free, as specified in the GCC" for further details please refer section V***
Inspections and Tests (GCC 23)		

33.	23.1	***There are no Special Conditions of Contract applicable to GCC Clause 23. for further details please refer section V***
Installations (GCC 24)		
34.	24.1	*There are no Special Conditions of Contract applicable to GCC Clause 24.* ***for further details please refer section V***
Operational Acceptance Test (GCC 26)		
35.	26.1	Operational Acceptance Testing shall be conducted in accordance with *Please refer section V*
Defect Liability (GCC 29)		
36.	29.1	For Software, exceptions or limitations to the Supplier's warranty obligations shall be as follows: *Please refer section V*
37.	29.3	The Supplier warrants that the following items have been released to the market for the following specific minimum time periods: *Please refer section V*
38.	29.4	The Warranty Period (N) shall begin from the date of Operational Acceptance of the System or Subsystem and extend for *Please refer section V*
39.	29.10	During the Warranty Period, the Supplier must commence the work necessary to remedy defects or damage within *Please refer section V*
Intellectual Property Rights Indemnity		
40.	30.1	***There are no Special Conditions of Contract applicable to GCC Clause 30.*** *Please refer section V*
Insurance (GCC Clause 31)		
41.	31.1	Not Applicable. *Please refer section V*
Related Services (GCC Clause 33)		

42.	33.1	Related services to be provided are: *Please refer section V*
Change Orders (GCC 34)		
43.	34.1	***There are no Special Conditions of Contract applicable to GCC Clause 34. Please refer the Section V***
Assignment (GCC 36)		
44.	36.1	Contract can be assigned - **No**
Liquidated Damages (GCC Clause 39)		
45.	39.1	Applicable rate: *0.2* Maximum deduction: is equal to the performance security. Note: 0.1 to 0.2 per cent per day of undelivered materials/good's value.

Procedure for Dispute Resolution (GCC Clause 45)		
46.	45.1	**Dispute Resolution** <u>For Contracts to be entered with foreign Contractor/ Service Provider</u>: *If the Supplier is foreign (including a Joint Venture when at least one partner is foreign), the Contract shall contain the following provision:* Arbitration proceedings shall be conducted in accordance with the rules of arbitration of *[select one of the following**: UNCITRAL / the International Chamber of Commerce (ICC) / the Arbitration Institute of the Stockholm Chamber of Commerce / the London Court of International Arbitration]**.* These rules, in the version in force at the time of the request for arbitration, will be deemed to form part of this Contract. **<u>For Contracts to be entered with nationals of Pakistan:</u>** If any dispute of any kind whatsoever shall arise between the Procuring Agency and the Supplier in connection with or arising out of the Contract, including without prejudice to the generality of foregoing, any question regarding its existence, validity, termination and the execution of the Contract– whether during developing phase or after their completion and whether before or after the termination, abandonment or breach of the Contract – the parties shall seek to resolve any such dispute or difference by mutual diligent negotiations in good faith within 7 (seven) days following a notice sent by one Party to the other Party in this regard. At future of negotiation the dispute shall be resolved through mediation and mediator shall be appointed with the mutual consent of the both parties.

		At the event of failure of mediation to resolve the dispute relating to this contract such dispute shall finally be resolved through binding Arbitration by sole arbitrator in accordance with Arbitration Act 1940. The arbitrator shall be appointed by mutual consent of the both parties. The Arbitration shall take place in Karachi and proceedings will be conducted in *English* language. The cost of the mediation and arbitration shall be shared by the parties in equal proportion however the both parties shall bear their own costs and lawyer's fees regarding their own participation in the mediation and arbitration. However, the Arbitrator may make an award of costs upon the conclusion of the arbitration making any party to the dispute liable to pay the costs of another party to the dispute. Arbitration proceedings as mentioned in the above clause regarding resolution of disputes may be commenced prior to, during or after delivery of goods. Notwithstanding any reference to the arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree that the Procuring Agency shall pay the Supplier any monies due to the Supplier.
Notices (GCC Clause 48)		
47.	48.1	— Procuring Agency's address for notice purposes: **Procurement Division, Logistics, Communications & Marketing Group, National Bank of Pakistan 3rd Floor, Head Office Building, Karachi. 021- 99220331, 021-38902647** —Supplier's address for notice purposes:

SECTION IX: CONTRACT FORMS

Form of Contract

THIS AGREEMENT made the day of 20____ between *[name and address of Procuring Agency]* of Pakistan (hereinafter called "the Procuring Agency") of the one part and *[name of Supplier]* of *[city and country of Supplier]* (hereinafter called "the Supplier") of the other part:

WHEREAS the Procuring Agency invited Bids for certain goods and related services, viz., *[brief description of goods and services]* and has accepted a Bid by the Supplier for the supply of those goods and related services in the sum of *[contract price in words and figures]* (hereinafter called "the Contract Price").

NOW THIS CONTRACT WITNESSETH AS FOLLOWS:

1. In this Contract words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Contract, In the event of any ambiguity or conflict between the Contract Documents listed below, the order of precedence shall be the order in which the Contract Documents are listed below:-

    a) This form of Contract;
    b) the Form of Bid and the Price Schedule submitted by the Bidder;
    c) the Schedule of Requirements;
    d) the Technical Specifications;
    e) the Special Conditions of Contract;
    f) the General Conditions of the Contract;
    g) the Procuring Agency's Letter of Acceptance; and
    h) [*add here: any other documents*]

3. In consideration of the payments to be made by the Procuring Agency to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Procuring Agency to provide the goods and related services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Procuring Agency hereby covenants to pay the Supplier in consideration of the provision of the goods and related services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Contract to be executed in accordance with their respective laws the day and year first above written.

Signed, sealed, delivered by__the____(for the Procuring Agency)

Witness to the signatures of the
Procuring Agency:
……

Signed, sealed, delivered by__the____(for the Procuring Agency) Witness to the signatures of the Supplier: ……

Performance Security (or guarantee) Form

To: *[name of Procuring Agency]*

WHEREAS *[name of Supplier]* (hereinafter called "the Supplier") has undertaken, in pursuance of Contract No. *[Reference number of the contract]* dated *[insert date]* to delivery *[description of goods and services]* (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a reputable bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Supplier a guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of *[amount of the guarantee in words and figures]*, and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limits of *[amount of guarantee]* as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the: *[insert date]*

Signature and seal of the Guarantors

_____

[name of bank or financial institution]

_____

[address]

_____

[date]

Integrity Pact

DECLARATION OF FEES, COMMISSION AND BROKERAGE ETC. PAYABLE BY THE SUPPLIERS OF GOODS, SERVICES & WORKS IN CONTRACTS WORTH RS.10.00 MILLION OR MORE

Contract Number: _____ Dated: _____
Contract Value: _____
Contract Title: _____

[Name of Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing [Name of Supplier] represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[Name of Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

[Name of Supplier] accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [Name of Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten time the sum of any commission, gratification, bribe, finder's fee or kickback given by [Name of Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.

_____ _____
[Buyer] [Seller/Supplier]

Declaration of Beneficial Owners

Declaration of Ultimate Beneficial Owners Information for Public Procurement Contracts over Fifty Million Pak Rupees as per PPRA S.R.O. 592(I) 2022

[In case of failure to provide the required information of the beneficial ownership by the company or submission of false or partial information, the procuring agency shall Blacklist the said company in accordance with rule 19 (1) (a) of Public Procurement Rules. 2004. and Reject the bid of the said company. The object or class of objects procured in contravention of any provision of S.R.O. 592(I) 2022 shall amount to mis-procurement]

l. Name
2. Father's Name/Spouse's Name
3. CNIC/NICOP/Passport No.
4. Nationality
5. Residential address
6. Email address
7. Date on which shareholding, control or interest acquired in the business.
8. In case of indirect shareholding, control or interest being exercised through intermediary companies, entries or other legal persons or legal managements in the chain of ownership or control, following additional particular to be provided:

Sr. No	**Particulars**	
1.	Name	
2.	Legal Form (Company/Limited Liability Partnership/Association of Persons/Single Member Company/Partnership Firm/Trust/Any Other Individual/Body/Corporate (to be specified).	
3.	Date of Incorporation/Registration	
4.	Name of Registering Authority	
5.	Business Address	
6.	Country	

7.	Email Address	
8.	Percentage of Shareholding, Control or Interest of BO in the Legal Person or Legal Arrangement.	
9.	Percentage of Shareholding, Control or Interest of the Legal Person or Legal Arrangement in the Company.	
10.	Identify of Natural Person who ultimately owns or Controls the Legal Person or Arrangement.	

9. Information about the Board of Directors (Details shall be provided regarding number of shares in the capital of the company as said opposite respective names).

Sr. No	**Particulars**	
1.	Name and Surname (In block letters)	
2.	CNIC Number (In case of foreigner, Passport Number)	
3.	Father's/Husband's name in full	
4.	Current Nationality	
5.	Any Other Nationality (ies)	
6.	Occupation	
7.	Residential Address in full or the Registered/Principal Office Address for the Subscribers other than the Natural Person.	
8.	Number of shares taken by Cash Subscriber (in figures and words)	
9.	Total Number of shares taken in	

	Figures and Words.	

10. Any other information incidental to or relevant to beneficial owner(s).

Name and signature

(Person authorized to issue notice on behalf of the company).

Annexure-1: SSDLC Checklist

Bidder to provide response with below options, where appropriate in SSDLC checklist.

1. True
2. False
3. N/A
4. Other (explain)

Application Security Review Checklist (Bidder to provide response)			Availability Response	Bidder Response
INSTRUCTIONS: Fill in all applicable sections.		Guide		
1.0	Application Components	Acceptable Criteria	(Yes/No)	
1.1	Are Application Components identified ?	Identify all application components (either individual or groups of source files, libraries, and/or executables) that are present in the application		
1.2	Are Application Dependencies identified ?	Identify all components that are not part of the application but that the application relies on to operate.		
1.3	Is the Application Architecture Defined ?	Identify a high-level architecture of the application.		
1.4	Are Application Business/Security Functions Identified ?	Identify all application components and defined in terms of the business functions and/or security functions they provide.		
2.0	Identification and Authentication			
2.1	Authentication of End-users Is the authentication mechanism implemented for end users?	If the application contains only public information then user authentication may not be required. A user Authentication mechanism must be implemented if the application contains Confidential, Sensitive Information with PII, Sensitive or Private information. The strength of the authentication mechanism must be commensurate with the risk of the application. e.g. two factor authentication for Customer facing internet applications or digital Certificates.		
2.2	Authentication for Administrator: Is the authentication mechanism implemented for administrator?	An authentication mechanism for Administrator must be implemented for the application regardless of which class of data the application contains. The administrator authentication mechanism must be at least as strong as the user authentication mechanism.		
2.3	Unique ID for user Does the application use a unique login ID for each user?	The generation of login IDs of users must be uniquely identifiable to user. If the answer is "No" it is unacceptable.		

2.4	Error Message for Failed login Attempts Does the application use a generic message for login attempts failures and account lockout?	All authentication controls fail securely. The error message for any failed login attempts and account lockout must be generic to prevent ID/Password guessing attacks. E.g. Invalid ID, Incorrect Password messages are not allowed. Log all authentication decisions. This should include requests with missing required information, needed for security investigations.		
2.5	User ID generation for Customer Are the identities generated based on the non-public information?	User identities should be generated without containing personal data e.g. personal data like ATM/Credit Card number, CNIC number. Email IDs can contain user names.		
2.6	Initial Password Does the application prompt to change the initial password?	Initial password should be pre-expired. Application should immediately prompt to change the initial password after the users first log into the application.		
2.7	Clear Text Password Password is never displayed on the screen in clear text (with the exception of one time use password resets).	All password fields do not echo the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete		
2.8	Static Password Strength Policy If static password are being used for authentication, is the strength policy being enforced to ensure password meets IT Security policy criteria, Password Expiration Notification, Password history, Maximum failed login attempts?	Password parameters shall be configured in accordance to NBP IT Security Policy as mentioned below: Password history should be maintained for at least 10 passwords. Password Should be hard to guess. It should not constitute with the common predict phrases like names, Tel Number, Date of Birth, Anniversary, same as user name etc. Account should be locked after 3-5 consecutive unsuccessful login attempts, release of locked account automatically after 30 minutes is recommended. User Level • Minimum 8 characters • Users should be forced to change on or before the expiry period of 45 days. • Account should be locked after 3-6 unsuccessful login attempts, and should only be unlocked upon receipt of request from valid user to the administrator. Privilege Level • Minimum 11 characters • Privilege / admin users should change their password on or before password expiry policy setting of 90 days.		
2.9	Static Password Rules If static password are being used, are the following password rules enforced? Password should be different from user name Password should not be easily guessable Password should not be blank	The strength of any authentication credentials are sufficient to withstand attacks that are typical of the threats in the deployed environment. Password should be different from user name Password should not be easily guessable passwords e.g. 12345678, asdfasdf, etc. Password should not be blank		

2.10	Session Inactivity Timeout Does the application enforce a session inactivity timeout?	Inactivity timeout for the users should be implemented to prevent unauthorized access of an active login session when the user is not present. Inactivity timeout period should be based on the application IS risk level which may be 5 to 15 minutes.		
2.11	Secure Authentication Protocol Is the application using the authentication based on the international standards	A secure mutual authentication protocol with a proper key management scheme to encrypt credentials (e.g. password) should be used. Examples are Kerberos, TLS. One time password or dynamic password can be sent in the clear over the network.		
2.12	Security Contexts Does the authentication server create unique security contexts for the authenticated users	secure session IDs / secure cookies / Kerberos tickets		
2.13	Dynamic Password System If a Dynamic password (one-time) system is used for authentication, it is approved by the Information Security and relevant stake holders.	All Dynamic password system must be reviewed by the Information Security before implementation.		
2.14	Digital Certificates and Certificate Authority (CA) If digital certificates are used, are they issued by approved CA?	Digital Certificates used by the application should be issued by approved CA authority/certificates provider e.g. VeriSign CA. Self-signed certificates can be used for testing purposes. PGP and point-to-point secure file transfer can be used where endpoint authentication is not required.		
2.15	Biometric Authentication if a Biometric Authentication mechanism is used by the application, is it approved by the IS?	Biometric authentication mechanism tend to be one-off solutions and are driven by business requirements (like ATM Authentication) therefore, they should be reviewed and approved by the IS to ensure they are secure.		
2.16	Two Factor Authentication if a two factor Authentication mechanism is used by the application, is it approved by the IS?	Two factor authentication or MFA should be reviewed by the IS/SME before the implementation.		
2.17	Single Sign-On (SSO) If the internet application is using shared authentication services, is it reviewed and approved by IS?	SSO or any shared authentication services should be reviewed by the IS/SME before the implementation.		
2.18	Logout Does the application allow users to completely log out from the application?	The application must provide the logout capability such that the user can completely log out of the application.		
2.19	Brute Force Attacks Is the resource governor controls in place to protect the application against vertical & horizontal brute forcing attacks?	The resource governor is in place to protect against vertical (a single account tested against all possible passwords) and horizontal brute forcing (all accounts tested with the same password e.g. “Password1”). A correct credential entry should incur no delay. Both these governor mechanisms should be active simultaneously to protect against diagonal and distributed Attacks.		
3.0	Authorization / Access Control /			

	Entitlement			
3.1	Authorization / Access Control / Entitlement If the application contains private or higher data, does the application provide mechanisms to control access based on the identity of the authenticated user.	Access control should be implemented and auditable. Users are given only those privileges necessary to perform their function. e.g. via entitlement profile / group / role base which are based on the Least Privilege. Access controls fail securely.		
3.2	Inactive / Obsolete Entitlement review Does the application support a mechanism to review inactive / obsolete entitlements	To ease entitlement review, it is beneficial if inactive/ obsolete entitlement can shown by the application		
3.3	Entitlement Review report Does the application provides the complete details of all users entitlement in form of a report? Security Administrator should have the ability to generate these reports per department / unit for periodic user entitlement review.	To ease entitlement review, application should generate the complete entitlement report of users for periodic entitlement review. High risk application should be able to provide the fine-grained entitlements. Verify that all access control decisions are being logged and all failed decisions are logged.		
3.4	Functional ID Management Does the application have a defined owner who is responsible for all aspects of the Functional IDs including usage, entitlement review and password management			
3.5	Access Control for Privileged Actions Does the application enforce access control for the following privilege actions? • Create, modify and delete user accounts and groups • Configure passwords or account lockout policy • Change passwords or certificates of user • Establish log sizes, fill threshold and behavior.	Access control on privileged access should be enforced to maintain system integrity. If least privilege cannot be enforced, compensating controls should be implemented to mitigate the risk (e.g. activity log review)		
3.6	Account management functions are account management functions secure.	All account management functions (such as registration, update profile, forgot username, forgot password, disabled / lost token, help desk or IVR) that might regain access to the account are at least as resistant to attack as the primary authentication mechanism.		
3.7	Re-Authentication is re-authentication required before any sensitive operations	Re-authentication is required before any application-specific sensitive operations are permitted. E.g. authenticating the customer again when conducting Financial Transaction or creating a beneficiary on an internet facing application		

3.8	Authenticity and Integrity of Authorization Data Is authorization data being stored on the client side (e.g. cookies, tickets) after the users get authenticated? If yes, is any mechanism being implemented to protect authorization data, prevent spoofing and maintain its integrity?	If authorization data is being stored on the client, it is important to ensure authorization data is protected/encrypted against unauthorized modification by the user. Ideally authorization data should be stored on the server to maintain data integrity.		
3.9	File and Directory Protection Is file and directory authorization enabled for user access control?	In addition to user entitlement, file and directory access control lists should be configured properly to protect the application's files against unauthorized access.		
3.10	Remote access System For internal application if non-NBP staff access this application remotely, is it over an approved solution which is reviewed and approved by IS?	All remote access to NBP systems / networks used by non-NBP staff (e.g. vendor) must be reviewed and approved by the IS.		
4.0	Data Confidentiality and Data Integrity			
4.1	Input Validation Does the application validate user inputs? Is input validation performed on the server or Client side?	Web Application that take data input can be exploited by the following attacks: buffer overflow, cross site scripting (XSS), SQL injection, code injection, denial of service and elevation of privileges. Input is validated to check for valid types, formats, lengths, and ranges and to reject invalid input. This validation is more critical if input filenames, URLs or user names are used for security decisions. Input validation must be performed on the server side instead on the client side to prevent it from being bypassed. Input validation should be enforced for the following: • Input from users • Parameter from URLs • Values from Cookies • Hidden fields to prevent SQL injection • Filter out character like single quotes, doNBPe quotes, slashes, back-slashes, semi colons, extended characters like NULL, carry return, new lines, etc. in all strings • Convert a numeric value to an integer or check whether it is an integer before parsing it into an SQL statement.		
4.2	Data Protection in Transit Is the sensitive or above category data protected during transmission in certain specific environments.	Identify the list of sensitive data processed by this application and there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). The transmission of data can take many forms including, but not limited to electronic file transfer (e.g. FTP), web traffic, e-mail, tapes, CDs, DVDs, Disk and so on. Transmission of sensitive PII should be encrypted. All cached or temporary copies of sensitive data are protected from unauthorized access or		

		purged/invalidated after the authorized user accesses.		
4.3	Input length Does the application limit the length of each user input field?	The length of every field should be limited		
4.4	Input Manipulation Does the application prevent Sensitive and above data from being passed in clear ?	Sensitive and above data especially authentication data must not be passed in clear text to prevent it from being manipulated by users.		
4.5	Content Cache Does the application prevent Sensitive and above data from being cached on user's local disk.	Sensitive and above data should not be cached on user's local disk. It could be accomplished in web application by implementation HTTP response header with: 'Prama:No-cach' for ASP or 'Cache-control: No cache' for JSP/Servlet.		
4.6	File Upload If the application supports file upload functionality, does it enforce the following a. Validate file extension/type, and file format. b. Run virus/malware scan on the uploaded file.	If data files are being uploaded to NBP servers from the external entity, the receiving server must have anti virus software to scan files before processing. The controls should be inplace to check the integrity of files such as Hashes. Only process the allowed/agreed file extensions. It is a sound practice to validate file extension / type, file format and run scan on the uploaded files, especially executables or other file type that can carry and propagate viruses.		
4.7	Data Protection in Storage Is data at the sensitive or above category protected in storage?	Sensitive and above category data must be protected/encrypted in storage and only accessible by respective users.		
4.8	Password Protection in Storage Is password data protected in storage	Account passwords are salted using a salt that is unique to each account and hashed before storing. All authentication credentials for accessing services external to the application are encrypted and stored in a protected location (not in source code).		
4.9	PII data Mask If the application has a feature to deliver or display an e-statement for customer account activities or to export production PII data, are customer account number/CNIC/credit card number partially masked?	Any combination of PII (personally Identifiable Information) that identifies an individual human being in a manner that would facilitate identity theft, credit fraud or other financial fraud must be protected against unauthorized access. Customer name or contact information in combination with CNIC number or tax number, passport number or account number is an example of Sensitive PII. Also note that when production data is exported for testing, PII data should be masked.		
5.0	Cryptography & Key Management			

5.1	Cryptographic Keys List all type of cryptographic keys such as symmetric, asymmetric, secure hash keys used in the solution. Describe their use scenarios and the security mechanisms associated with each cryptographic algorithm used	if encryption is used for authentication, data protection, key management, digital signature or other purposes, all cryptographic keys including their type, cryptographic algorithms and key length and secure hash algorithm must be listed as a pre-requisite for key management assessment. For instance, an application may implement 2048-bit RSA digital certificates for user authentication and key management, 128-bit AES for data protection in transit, and SHA-2 for password protection.		
5.2	Cryptographic Algorithms and Key lengths Do all cryptographic keys comply with current market standards/requirements? (AES/3DES/RC4, SHA-2/256, RSA etc.) and key length?	Security of the data encryption shall depend on secrecy of the key, not secrecy of the algorithm. All the cryptographic algorithms and key length being used must be validated against FIPS 140-2 or an equivalent current market standards/requirements, Symmetric keys: 168-bit 3DES, 128 AES Asymmetric keys: 2048-bit RSA or 256-bit ECDSA or ECDH Source hash: SHA2 (i.e. SHA-256/384/512)		
5.3	Key Generation & Management Are all cryptographic keys randomly generated using approved Random Number Generator? What type of random number generator is used by the application?	All cryptographic keys must me randomly generated by approved random number generator (e.g. as per NIST FIPS 140-2), also define how cryptographic keys are managed (e.g., generated, distributed, revoked, expired)		
5.4	Key Data Display if a manual key entry process is used, do utilities used to load or enter keys or key components prevent the display of the data loaded or entered in the clear?	Distribute the key between multiple custodians and prevent to display the keys in clear during entry		
5.5	Key Renewal Frequency Do all cryptographic keys have a defined renewal frequency period to comply with	Cryptographic keys should be changed on a periodic basis commensurate with the frequency of key use or exposure to eavesdropping or unauthorized access. E.g. • Key encryption: At least once per month (automated) • Master keys or symmetric keys for authentication or key management : at least once per year (if manual renewal) • Cryptographic keys that cannot be renewed should have a pre-defined expiration period (e.g. 3 years of PIN generation keys)		
5.6	Key Protection in Storage Are all symmetric and asymmetric (private) keys, except public keys, encrypted and stored in a hardware or software cryptographic module with proper access control?	Cryptographic keys except public keys, must be encrypted in storage with proper access control. Access control must be prevent unauthorized access.		

5.7	Hard-coding Cryptographic Keys Does the application prevent any encryption keys or passkey being included in the source code or configuration files?	• Hard coded keys that are manually set into code or part of the application and cannot be changed are not acceptable as the keys are known to developers and all instances of the application should use the same set of keys. • Cryptographic keys being coded as the default should be configured and changeable during installation or configuration. • if Cryptographic keys are hardcoded they cannot be changed. Therefore, not acceptable.		
5.8	Certification Validation When digital certificates are used for the digital signature or authentication, is an up-to-date certification revocation list (CRL) used to verify the validity of the CA's and user's / server's certificates if an on-line certificate validation mechanism via Online Certificate Status Protocol (OCSP) or Server-based Certificate Validation Protocol (SCVP) is not available?	• When an online certificate validation protocol such as OCSP or SCVP is not supported. CRLs must be made available for servers to client's certificates or for the clients to server's certificate if certificates are used for digital signature or authentication.		
5.9	CRL renewal When a CRL is used for certification validation, are cached copies of CRLs updated regularly? If so, please describe the frequency (e.g. once per day). Is the frequency of update commensurate with the associated risk of the application.	• CRL (Certificate Revocation Lists) must be updated periodically.		
5.10	Key Recovery Compliance if the application is subject to supervisory or data retention requirements such as SBP - psd/2014/C3-Annex or section 7 of PS&EFT Act 2007 or any other key recovery requirements, is there a key recovery process to fulfill the regulatory requirements?	• To comply with NBP policy or other regulatory requirements, key recovery must be enforced, such as encrypted transactional messages or data can be decrypted and recorded for regulatory compliance, log all Cryptographic module failures		
5.11	Unique Key Does each cryptographic key have a unique application domain? For each party, there should be as many different keys as there are different cryptographic functionalities.	• Any particular key should be used for one particular purposes (e.g. signing, data encryption, Key encryption etc.) • Keys used for in production environment must not be used for development or testing.		
6.0	Error Handling & Audit Logging			

6.1	Auditing and Events Does the application have an auditing capability across application layers? Depending on the risk of the application, are audit logs and alerts of unauthorized access maintained?	The answer should be "Yes" since to comply with the NBP IT policy section 2.3.5.5 Logging is performed before executing the transaction. If logging was unsuccessful (e.g. disk full, insufficient permissions) the application fails safe, this is for when integrity and non-repudiation are a must. Following significant events should be available for review: • ID Management (Create, Delete, Modify, Suspend, Resume) • Successful / Unsuccessful user login attempt • Account Lock out • Account Lock/Unlock • Group Creation • Creation or modification of application roles/ profiles • Creation/modification/deletion of user rights • Password Forget • Password Resets • Password Change • Change in Application/System security configuration • Alarms associated with a firewall or IDS/IPS • Financial Transaction or Sensitive PII data • Security Validation failure • Session Management failure • Application/Service Start/Stop • Suspicious/Fraud and other criminal activities		
6.2	Audit Events contents Does the individual audit event contain the necessary attributes?	Each log entry needs to include sufficient information for the intended subsequent monitoring and analysis. The application logs must record "when, where, who and what" for each event. All auditable events must give enough information to trace the event to a particulars but not limited to the following: • Unique log identifier • The user ID or the process ID of the event • System, application, module or component • Data and Time of the event • Application address e.g. IP address or machine name and port number • Resource ID e.g. window, url, page, form, method • Service Protocol • Source Address e.g. user/service IP address • Device Identifier e.g. IMEI, MAC • User, object Identity • Type of the event • Log Level • Success or failure of an event • Starting and ending time of access to the application • Description		

6.3	Admin activities Does security Administration activities for this system are logged and traceable to User ID?	To achieve the non-repudiation all the generic IDs should be escrowed and only accessible in case of emergency, each user must have its own ID and guarantees that an action can be proven to have originated from specific person.		
6.4	Audit Log Protection Are audit logs in store and during transmission, protected from unauthorized deletion, modification and disclosure? i.e. Administrator should not have the ability to modify / edit the logs	Audit Logs must be protected against unauthorized access to ensure its integrity and maintain accountability. The application does not output error messages or stack traces containing sensitive data that could assist an attacker, including Session ID and personal information.		
6.5	Audit Log File Configuration Can the audit log files be configured for log size and rollover to prevent log file data loss and a denial of service attack?	Audit Logs should be automatically roll over unless it can be ensured that the audit logs have been backed up or archived. Audit log file size should be configurable to prevent a denial of service attack or application handles log size issue automatically. Rollover must always be configurable.		
6.6	SIEM Integration Is application capable to integrate with SIEM	Application should be able to integrate with SIEM solution. SIEM is available which allows the analyst to search for log events based on combinations of search criteria across all fields in the log record format supported by this system.		
6.7	Audit Log Notification Are administrators warned when the audit logs are nearly full?	It is desirable to have a mechanism to warn administrator when the audit logs are nearly full to prevent an application from shutting down, from a denial of service or from overriding previous logs.		
6.8	Reports Does the application have an ability to generate custom audit reports based on the criteria specified by the log reviewer?	It is desirable to have a capability to generate audit reports based on a number of criteria specified by the log reviewer.		
7.0	Security Administration			
7.1	Functional ID If the application is using functional IDs (e.g. root in Linux/Unix, Administrator in Windows), are they protected against unauthorized usage?	It is important to list any functional Ids that exist and if any internal application or third party controls can be placed on the system to decrease the privileges associated with these accounts. Also controls should be in place for any system functional IDs to prevent unauthorized usage. In general, the existence of all power administration IDs is not desirable.		
7.2	Service Accounts Are service/database ids only used by the applications and not used by individual users or other processes	The application backend IDs such as database, service accounts are restricted and only allowed by the application. These accounts would not be accessible by any individual users.		
7.3	Separation of Roles Does the application split administration privileges into several accounts (e.g. system administration, Security Administration)?	According to the principle of least privilege it is desirable for administrative accounts to have the least privilege needed to perform a particular function. It is describable to have separate administrative roles to perform system management, security management and audit. If separation of roles cannot be enforced, then the		

		application must have provisions (e.g. auditing to ensure the accountability of the privileged accounts.		
7.4	Administrator's Conflict of Interest Does the application prevent a security administrator from performing transactions or administrative functions for themselves that conflict with this role?	The application should not allow security administrator to create or modify user accounts for themselves. In case there is a business requirement to allow such action, then an independent verification or maker/checker process must be implemented and all such actions must be audited.		
7.5	Maker/Checker for Administrative Actions Does the application support maker/checker or dual-control for administrative actions (e.g. account creation / modification, entitlement management).	It is describable to have internal maker/checker or dual-control for administration actions such as account creation/modification and entitlement management. When maker/checker or dual-control cannot be implemented, an independent verification process must be enforced.		
8.0	System Security and Availability			
8.1	Application Identity Is the application or web server running as a non-privileged user (e.g. non-root or non-administrator)?	If possible, the application or web server should run as non-privileged user, especially when this is a customer facing application. This provision should be implemented to reduce/control damage in case the application is compromised.		
8.2	Application Integrity Is there a mechanism to protect application configuration stores and maintain the integrity of critical application files?	It is important to protect application configuration stores and critical files with access control. This include all share folder for data and system files.		
8.3	BCP/DR Does the application support redundancy or replication for continuity of business or automatic fail-over?	Automatic fail-over is commonly required for mission-critical applications for high availability. However, some low criticality application may not have a BCP/DR requirement or manual process (last updated data restoration on contingency server). It is a business decision to determine whether it is required or not.		
8.4	DDOS attack Are controls in place to prevent a denial of service (DOS) attack on this system?			
9.0	Network Architecture and Perimeter Security			
9.1	Perimeter Security For Applications deployed in the DMZ, does the application prevent unauthenticated users from the Internet from accessing a server on our intranet?	For Internet applications, unauthenticated users must not be allowed to directly access the server or Intranet to prevent hackers from exploiting vulnerabilities on the server that would first compromise the server and then internal infrastructure. Users must be authenticated on a server in the DMZ (e.g. a web or VPN server) before interacting with another server on intranet. For B2B application, B2B server/devices must be placed in the DMZ to perform authentication.		

9.2	3-Tier Architecture Does the application support at least 3-Tier Architecture (e.g. web server, application server and backend server/database) to protect data from being directly accessed from the web server in the DMZ.	For Internal web applications, especially financial application or application that provide personal data, it is desirable to have at least a 3-tier architecture (3 tiers may include the tiers of web server, application server and backend server or database server)to protect the backend server/database from being directly accessed from the web server and being compromised.		
9.3	Persistent Storage on the DMZ if this is an Internet-based application, does the application prevent Confidential and above data from being persistently stored on a system in the DMZ?	Confidential and above category data should not be persistently stored on a system in the DMZ. i.e. Persistently stored means storage beyond the session lifetime.		
9.4	System-to-System Authentication Does the application support system-to-system authentication or the authentication at the application layer for communication between any two servers to prevent unauthorized access?	System-to-system authentication or authentication at the application layer should be implemented for communication between any two servers to prevent unauthorized access. Network access control such as SSL or IPsec could be used as a compensating control if system-to-system authentication or authentication at the application layer is not implemented. Note that IPsec is consider as the last resort.		
10.0	Session Management			
10.1	Session Management Does the authentication server(s) implements a session management mechanism to manage active login sessions and to prevent spoofing/masquerading?	Session management for this case is used to record the states of active login sessions and to retire inactive sessions when they time out. Session management should have the following properties: • Unique session identification • Session Identification that are protected in transit and in storage against unauthorized access. • An inactivity time out mechanism		
10.2	Application Logout Does the application have a logout functionality on every screen that is available for authenticated user?	When a user logs out, the application must completely log the user out and prevent the user from accessing pages or information that is available to active authenticated users.		
10.3	Session Identifier Generation Does the application generate session identifiers (IDs) with a sound pseudo-random number generator?	Session management is required for web applications because they are based on the stateless HTTP protocol. Therefore, session management is critical to the overall security of web applications. A sound session management scheme should be able to generate unique and unpredictable session IDs, restrict session lifetime, and protect session IDs.		
10.4	Session State Store Does the application protect its session state store against unauthorized access?	The session state store can be local or remote. Session state data should be protected against eavesdropping and unauthorized access. If session state store is remote then the data in transit should be encrypted with a secure protocol such as SSL or IPsec and the data in		

		store should be protected against unauthorized access.		
10.5	Session Lifetime Does the application restrict session lifetime and enforce the maximum login period for a session?	Prolonged session lifetime would increase the risk of session hijacking and reply attacks. Therefore the application should restrict session lifetime to reduce the risk. IS Policy requirements of inactive user session • 5 minutes for Critical System that are classified as sensitive; • 10-15 minutes for other classified systems based on business need		
10.6	Session Identification Passage Does the application prevent session identifiers from being passed over unencrypted channels?	If session IDs are used to track session states, then session IDs or cookies containing session IDs should be passed via encrypted channels (e.g. SSL/TLS) to prevent eavesdropping.		
10.7	Session Identifier Manipulation Does the application prevent users from manipulating session identifiers that are being passed in query string or from fields?	Session IDs should not be passed via query string or from fields because they can be easily modified by the users in an attempt to impersonate other users.		
10.8	Session Cookies Does the application encrypt session cookies?	Session (authentication) cookies should be encrypted to prevent session cookies from being stolen. Session cookie encryption along with SSL/TLS can mitigate the risk of cross-site scripting (XSS) attacks. Session cookies values that are created in insecure session should not be inherited in secure session cookies.		
10.9	Session Cookies Validation If session cookies are used by application, does the application validate the cookies before granting access to protected pages?	Cookies that contain Restricted or authentication data must be marked secure, so that they are sent only over encrypted channel, namely SSL/TLS. Cookies that contain Sensitive PII must be marked secured when transmitting via non-NBP manage infrastructures.		
10.10	Secure Cookies If the application uses cookies containing Sensitive or Higher information, are the cookies marked secured so that the cookies are sent only over encrypted channels AND is the cookies content encrypted using approved method?	Cookies that contain Sensitive+ data must be marked secure, so that they are sent only over encrypted channels, namely SSL/TLS. Cookies that contain Sensitive PII must be marked secured when transmitting via non-NBP managed infrastructures.		
11.0	Database Access			

11.1	Database Authentication Does the application server utilize the database authentication to directly connect to the database instead of user account authentication at the application level?	The Application Server may use a database account or an application account to establish the database connectivity. When the user accounts in the Application are tightly coupled with the database accounts, the database is accessible by all legitimate users on the platform. To enforce the principle of least privilege, it is more secure for application to use separate database accounts for DB authentication. In case where a user account on the Application server used to access the database, a least privileged account should be created.		
11.2	Database Password Protection in Storage Does the application protect/encrypt database connection strings (e.g. passwords) in local storage?	Database connection string contain authentication data and therefore must be encrypted in storage. Encrypted connection string and encryption keys must be protected. The function of decrypting connection string should be a standalone utility to prevent the connection string from being decrypted and display in the clear. Instead, it should be embedded into or fully integrated within the application.		
11.3	Database Password Protection in Transit Does the application enable/implement a secure protocol (e.g. SSL/TLS) to protect database passwords in transit?	If database connection string contains passwords it must be encrypted in the transit. In general, most database system support a secure protocol (e.g. SSL / TLS) for this purpose. When a secure protocol cannot be enabled or applied. IPsec or other secure protocol can be considered as a last resort for host-to-host encryption.		
12.0	Legal / Regulatory Compliance, Management Approval & Awareness			
12.1	Additional Legal or Regulatory Requirements Does the application comply with all regulatory / local laws which are not included in the Information Security policy.	Each and every application must comply with Legal/Regulatory/IS requirements.		
12.2	Banner Text Approval Is the Legal Department approved banner text, when supported by the application, displayed at all entry points where a user initially signs on?	If there is a need to support banner tax, legal-approved banner text must be displayed at all entry points where a user initially signs on either from local or remote access.		
13.0	Application Configuration and IS Processes			

13.1	Information Classification Has the information been classified in accordance with NBP Information Standards?	NBP TBML system(s) assets must be given a classification level in accordance with the NBP approved classification standard. • Confidential Information that is considered to be very sensitive to business and is intended for internal use only by following the need to know principle. Unauthorized disclosure of this level of information could seriously and negatively impact bank's reputation and may cause significant business loss. • Sensitive Information that requires a higher level of protection than normal from unauthorized disclosure or alteration. Unauthorized disclosure / alteration of such information may negatively impact bank's reputation or can cause legal implications. • Private Proprietary information that is being developed for NBP internal use and being shared among the NBP employees only. Property of NBP and disclosure of such information could affect the NBP business or employees. • Public Information either collected from public sources or being produced for public review. Disclosure of such information will not have an impact to NBP business & employees.		
13.2	Inherent Risk of the Application Has an inherent risk analysis been completed by the business during the definition phase of the project?	IS Risk Assessment is a mandatory requirement, Risk Assessment lifecycle must be completed in coordination of IS Risk team.		
13.3	Vendor Support Product Is the application software supported by an approved vendor?	Application vendor must be in the NBP's approved vendor list.		
13.4	Default Access Capability Are all default access capabilities (including passwords) removed, disabled or protected to prevent their unauthorized use?	No default ID should be used or enabled. Default IDs should be renamed and password split and escrowed with IS		
13.5	Vulnerability Assessment If required, has the application undergone all of the Application vulnerability Assessment and remediated all security findings as specified in the VA process.	If VA is required for this application, the required VA (Internal or External) must be performed and all security findings with the medium and High risk level must be remediated with the timeframe specified in the VA process.		
13.6	Masking Data Is sensitive PII information masked within the application whenever possible (displaying as well as printing)?	By the GLBA act, financial institutions must protect the security and confidentiality of customer's nonpublic personal Information (NPI). When NPI is being displayed or printed, it should be partially masked and only the last four digits can be displayed or printed for identification or verification.		

13.7	Configuration location are application configuration files protected from unauthorized access?	All security-relevant configuration information is stored in locations that are protected from unauthorized access.		
13.8	Configuration Error is application capable of handling configuration errors?	If the application cannot access its security configuration, all access to the application should be denied and do not allow access using default configuration.		
13.9	Audit Configuration Changes is auditing enabled to track application configuration changes?	All changes to the security configuration settings managed by the application are logged in the security event log.		
13.10	Fax Are automated or manual fax processes used in connection with the transection of data to/from the system? If yes describe the controls around the fax process.	If sensitive or above information must be sent over Fax, specific procedures and guidance must be created and followed to mitigate the risk. Fax cannot support user authentication nor data confidentiality. Manual authentication of the source and verification of the data may to be conducted to mitigate the risk and such action may need to be logged/recorded for accountability.		
14.0	Compliance			
14.1	3rd Party Solution is it certified by PCI, Common Criteria?	The solution related to Card processing must be certified by PCI, Common Criteria min Level 3+.		
14.2	Have any non-compliance being found as a result of this review? If True, provide corrective action plan and/or RA numbers in the "Open Issues and Approvals" TAB of this document			

Web Secure Coding Checklist (Bidder to provide response) *Bidder should complete this checklist in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.*		*Availability Response*	*Bidder Response*
1.0 Application Verification			
1.1	The integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes.		
2.0 Authentication			
2.1	All pages and resources require authentication except those specifically intended to be public.		
2.2	All password fields do not display the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.		
2.3	If a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.		
2.4	All connections to external systems that involve sensitive information or functions are authenticated.		

2.5	The forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.		
2.6	The username enumeration is not possible via login, password reset, or forgot account functionality.		
2.7	All authentication controls are enforced on the server side.		
3.0 Session Management			
3.1	The framework's default session management control implementation is used by the application.		
3.2	Sessions are invalidated when the user logs out.		
3.3	Sessions timeout after a specified period of inactivity.		
3.4	Sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		
3.5	All pages that require authentication to access them have logout links.		
3.6	The session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.		
3.7	The session id is changed on each login.		
3.8	The session id is changed on re-authentication.		
3.9	The session id is changed or cleared on logout.		
3.10	Only session ids generated by the application framework are recognized as valid by the application.		
3.11	Authenticated session tokens are sufficiently long and random to withstand attacks that are typical of the threats in the deployed environment.		
3.12	Cookies which contain authenticated session tokens/ids have their domain and path set to an appropriately restrictive value for that site. The domain cookie attribute restriction should not be set unless for a business requirement, such as single sign on.		
3.13	Verify that authenticated session tokens using cookies sent via HTTP, are protected by the use of "HttpOnly".		
3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and a strict transport security headers are present.		
3.15	Verify that the application does not permit duplicate concurrent user sessions, originating from different machines.		
4.0 Access Control			
4.1	Users can only access URLs for which they possess specific authorization.		
4.2	Direct object references are protected, such that only authorized objects are accessible to each user.		
4.3	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
4.4	Directory browsing is disabled unless deliberately desired.		
4.5	The same access control rules implied by the presentation layer which are enforced on the server side, such that controls and parameters cannot be re-enabled or re-added from higher privilege users.		

4.6	All user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.		
4.7	Verify the system can protect against aggregate or continuous access of secured functions, resources, or data. For example, possibly by the use of a resource governor to limit the number of edits per hour or to prevent the entire database from being scraped by an individual user.		
4.8	There is a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.		
4.9	Verify that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
4.10	Limitations on input and access imposed by the business on the application (such as daily transaction limits or sequencing of tasks) cannot be bypassed.		
4.11	All access controls are enforced on the server side.		
5.0 Input Validation			
5.1	The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.		
5.2	All input validation failures result in input rejection.		
5.3	All input validation or encoding routines are performed and enforced on the server side.		
5.4	Single/Centralized input validation control is used by the application for each type of data that is accepted.		
5.5	All input validation failures are logged.		
5.6	All input data is canonicalized for all downstream decoders or interpreters prior to validation.		
5.7	The runtime environment is not susceptible to SQL,LDAP,OS,XML Injection, or that security controls to prevent the Injection attacks.		
5.8	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
5.9	If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, verify that security sensitive fields such as accountBalance,role, password etc. are protected from malicious automatic binding.		
5.10	The application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)		
6.0 Output Encoding/Escaping			
6.1	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
6.2	All output encoding/escaping controls are implemented on the server side.		
6.3	Output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.		

6.4	All untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.		
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or are escaped properly.		
6.6	All untrusted data that are output to any interpreters not specifically listed above are escaped properly.		
6.7	For each type of output encoding/escaping performed by the application, there is a single/centralized security control for that type of output for the intended destination.		
7.0 Cryptography Requirements			
7.1	All cryptographic functions used to protect secrets from the application user are implemented on server side.		
7.2	All cryptographic modules fail securely.		
7.3	Access to any master secret(s) is protected from unauthorized access (a master secret is an application credential stored on disk which is used to protect access to security configuration information).		
7.4	Password hashes are salted uniquely when they are created.		
7.5	Cryptographic module failures are logged.		
8.0 Error Handling and Logging			
8.1	All logging controls are implemented on the server.		
8.2	Verify security logging controls, provide the ability to log both success and failure events that are identified as security-relevant.		
8.3	All events that include untrusted data will not execute as code in the intended log viewing software.		
8.4	Single logging implementation is used by the application.		
8.5	Application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.		
8.6	All code implementing or using error handling and logging controls is not affected by any malicious code.		
9.0 Data Protection			
9.1	All forms containing sensitive information have disabled client side caching, including autocomplete features.		
9.2	All sensitive data is sent to the server in the HTTP message body (i.e., URL/GET parameters are never used to send sensitive data).		
9.3	All cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		
9.4	There is a method to remove each type of sensitive data from the application at the end of its required retention period.		
10.0 Network Communication Security			
10.1	A path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each certificate is valid.		
10.2	Failed SSL/TLS connections do not fall back to an insecure connection.		

10.3	SSL/TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		
10.4	SSL/TLS connection failures are logged.		
10.5	Certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.		
10.6	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
10.7	There is a single standard SSL/TLS implementation that is used by the application that is configured to operate in an approved mode of operation		
11.0 HTTP Security			
11.1	"Redirect" (i.e. 302 Object moved) do not include unvalidated data. Form data redirect may be hijacked if compromised or mismanaged. If it is redirected to a site in a different domain, the users cannot tell whether the site is trusted or not before sensitive data contained in the form are submitted. Therefore, we recommend to NOT implement "redirect" when accepting sensitive information from user forms.		
11.2	The application accepts only a defined set of HTTP request methods, such as GET and POST.		
11.3	Every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).		
11.4	The HTTPOnly flag is used on all cookies that do not specifically require access from JavaScript.		
11.5	The secure flag is used on all cookies that contain sensitive data, including the session cookie.		
11.6	HTTP headers in both requests and responses contain only printable ASCII characters and do not expose detailed version information of system components.		
11.7	The HTTP header, X-Frame-Options is in use for sites where content should not be viewed in a 3rd-party X-Frame. A common middle ground is to send SAME ORIGIN, meaning only websites of the same origin may frame it.		
11.8	The application generates a strong random token as part of all links and forms associated with transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
11.9	The HTTP header can be easily manipulated by an attacker and must not be used for security decisions.		

Web Secure Coding Checklist (Bidder to provide response) *Bidder should complete this checklist in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.*		*Availability Response*	*Bidder Response*
1.0 Application Verification			
1.1	The integrity of interpreted code, libraries, executables, and configuration files is verified using checksums or hashes.		
2.0 Authentication			
2.1	All pages and resources require authentication except those specifically intended to be public.		
2.2	All password fields do not display the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.		
2.3	If a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.		
2.4	All connections to external systems that involve sensitive information or functions are authenticated.		
2.5	The forgotten password function and other recovery paths do not reveal the current password and that the new password is not sent in clear text to the user.		
2.6	The username enumeration is not possible via login, password reset, or forgot account functionality.		
2.7	All authentication controls are enforced on the server side.		
3.0 Session Management			
3.1	The framework's default session management control implementation is used by the application.		
3.2	Sessions are invalidated when the user logs out.		
3.3	Sessions timeout after a specified period of inactivity.		
3.4	Sessions timeout after an administratively-configurable maximum time period regardless of activity (an absolute timeout).		
3.5	All pages that require authentication to access them have logout links.		
3.6	The session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.		
3.7	The session id is changed on each login.		
3.8	The session id is changed on re-authentication.		
3.9	The session id is changed or cleared on logout.		
3.10	Only session ids generated by the application framework are recognized as valid by the application.		
3.11	Authenticated session tokens are sufficiently long and random to withstand attacks that are typical of the threats in the deployed environment.		
3.12	Cookies which contain authenticated session tokens/ids have their domain and path set to an appropriately restrictive value for that site. The domain cookie attribute restriction should not be set unless for a business requirement, such as single sign on.		

3.13	Verify that authenticated session tokens using cookies sent via HTTP, are protected by the use of "HttpOnly".		
3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and a strict transport security headers are present.		
3.15	Verify that the application does not permit duplicate concurrent user sessions, originating from different machines.		
4.0 Access Control			
4.1	Users can only access URLs for which they possess specific authorization.		
4.2	Direct object references are protected, such that only authorized objects are accessible to each user.		
4.3	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
4.4	Directory browsing is disabled unless deliberately desired.		
4.5	The same access control rules implied by the presentation layer which are enforced on the server side, such that controls and parameters cannot be re-enabled or re-added from higher privilege users.		
4.6	All user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.		
4.7	Verify the system can protect against aggregate or continuous access of secured functions, resources, or data. For example, possibly by the use of a resource governor to limit the number of edits per hour or to prevent the entire database from being scraped by an individual user.		
4.8	There is a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.		
4.9	Verify that the application or framework generates strong random anti-CSRF tokens unique to the user as part of all high value transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
4.10	Limitations on input and access imposed by the business on the application (such as daily transaction limits or sequencing of tasks) cannot be bypassed.		
4.11	All access controls are enforced on the server side.		
5.0 Input Validation			
5.1	The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.		
5.2	All input validation failures result in input rejection.		
5.3	All input validation or encoding routines are performed and enforced on the server side.		
5.4	Single/Centralized input validation control is used by the application for each type of data that is accepted.		
5.5	All input validation failures are logged.		
5.6	All input data is canonicalized for all downstream decoders or interpreters prior to validation.		

5.7	The runtime environment is not susceptible to SQL,LDAP,OS,XML Injection, or that security controls to prevent the Injection attacks.		
5.8	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
5.9	If the application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, verify that security sensitive fields such as accountBalance,role, password etc. are protected from malicious automatic binding.		
5.10	The application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)		
6.0 Output Encoding/Escaping			
6.1	All untrusted data that are output to HTML (including HTML elements, HTML attributes, JavaScript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.		
6.2	All output encoding/escaping controls are implemented on the server side.		
6.3	Output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.		
6.4	All untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.		
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or are escaped properly.		
6.6	All untrusted data that are output to any interpreters not specifically listed above are escaped properly.		
6.7	For each type of output encoding/escaping performed by the application, there is a single/centralized security control for that type of output for the intended destination.		
7.0 Cryptography Requirements			
7.1	All cryptographic functions used to protect secrets from the application user are implemented on server side.		
7.2	All cryptographic modules fail securely.		
7.3	Access to any master secret(s) is protected from unauthorized access (a master secret is an application credential stored on disk which is used to protect access to security configuration information).		
7.4	Password hashes are salted uniquely when they are created.		
7.5	Cryptographic module failures are logged.		
8.0 Error Handling and Logging			
8.1	All logging controls are implemented on the server.		
8.2	Verify security logging controls, provide the ability to log both success and failure events that are identified as security-relevant.		
8.3	All events that include untrusted data will not execute as code in the intended log viewing software.		
8.4	Single logging implementation is used by the application.		

8.5	Application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.		
8.6	All code implementing or using error handling and logging controls is not affected by any malicious code.		
9.0 Data Protection			
9.1	All forms containing sensitive information have disabled client side caching, including autocomplete features.		
9.2	All sensitive data is sent to the server in the HTTP message body (i.e., URL/GET parameters are never used to send sensitive data).		
9.3	All cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).		
9.4	There is a method to remove each type of sensitive data from the application at the end of its required retention period.		
10.0 Network Communication Security			
10.1	A path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and each certificate is valid.		
10.2	Failed SSL/TLS connections do not fall back to an insecure connection.		
10.3	SSL/TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		
10.4	SSL/TLS connection failures are logged.		
10.5	Certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.		
10.6	All connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.		
10.7	There is a single standard SSL/TLS implementation that is used by the application that is configured to operate in an approved mode of operation		
11.0 HTTP Security			
11.1	"Redirect" (i.e. 302 Object moved) do not include unvalidated data. Form data redirect may be hijacked if compromised or mismanaged. If it is redirected to a site in a different domain, the users cannot tell whether the site is trusted or not before sensitive data contained in the form are submitted. Therefore, we recommend to NOT implement "redirect" when accepting sensitive information from user forms.		
11.2	The application accepts only a defined set of HTTP request methods, such as GET and POST.		
11.3	Every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).		
11.4	The HTTPOnly flag is used on all cookies that do not specifically require access from JavaScript.		
11.5	The secure flag is used on all cookies that contain sensitive data, including the session cookie.		

11.6	HTTP headers in both requests and responses contain only printable ASCII characters and do not expose detailed version information of system components.		
11.7	The HTTP header, X-Frame-Options is in use for sites where content should not be viewed in a 3rd-party X-Frame. A common middle ground is to send SAME ORIGIN, meaning only websites of the same origin may frame it.		
11.8	The application generates a strong random token as part of all links and forms associated with transactions or accessing sensitive data, and that the application verifies the presence of this token with the proper value for the current user when processing these requests.		
11.9	The HTTP header can be easily manipulated by an attacker and must not be used for security decisions.		

API Security Review Checklist (Bidder to provide responses, If applicable)			Availability Response	Bidder Response
INSTRUCTIONS: Fill in all applicable sections.		Guide		
1.0	Authentication & Authorization	Acceptable Criteria	(Yes/No)	
1.1	Use secure authentication mechanism	Don't use basic authentication with plaintext credentials e.g. plaintext password in URL parameter etc. Apply standard & secure authentication such as JWT tokens with dynamic mechanism per session/per request, OAuth 2.0, or public/private API keys combination.		
1.2	Ensure secure storage of passwords, API tokens & keys	Store API tokens/keys in secure key vaults via secure mechanism such as Windows Local Security Authrority so that tokens & keys remain secure including the config file data.		
1.3	Ensure encryption of sensitive data & tokens in transit and at rest	Sensitive data including credentials must be encrypted in transit and at rest. Use transport layer security protocols and strong encryption algorithms e.g. RSA, AES-256 etc.		
1.4	Never place the credentials in source code	Plaintext credentials or hashes must not be placed in source code to avoid misuse & brute force attacks by adversaries.		
1.5	Configure maximum login retries following the IS policy of organization	For NBP assets, 5 maximum retries should be allowed before the account gets locked. It prevents brute force attacks.		
2.0	Access Security			
2.1	Use HTTPS insead of HTTP	Implement SSL based communication over API connections.		
2.2	Display as minimum information as possible in you API request/response	Don't rely on client side to filter data; Avoid using generic methods such as to_json() and to_string(). Instead, cherry-pick specific properties & data you really want to return.		
3.0	Input Security			

3.1	Sensitive data protection in URL	Don't use any sensitive data (credentials, passwords, security tokens, and/or API keys) in the URL but use standard Authorization header.		
3.2	Use appropriate HTTP method according to the operation	Use GET (read), POST (create), PUT/PATCH (replace/update), and DELETE (to delete a record) methods appropriately in API communication. Respond with *405 Method Not Allowed* if the requested method is not appropriate for the requested resource.		
3.3	Ensure content validation controls for input security	Content Validation for Request: To validate the content type of response, use Accept header in HTTP request (Content Negotiation) to allow only the supported formats (e.g., application/xml, application/x-www-form-urlencoded, multipart/form-data, application/json etc.). Content Validation for SQL injection, RCE and XSS: Validate the user-submitted content for SQL injection, Remote Code Execution, and Cross-Site Scripting (XSS).		
3.4	Ensure Secure Coding Practice	Remove unused dependencies, unnecessary features, components, files, and documentation. Run depenciy check tools such as OWASP Dependency check.		
3.5	Make trusted updates of packages	Always check for trusted sources. Get the packages for your application with authorized signature so that no malicious component is included in the package.		
3.6	Apply caching and rate limiting	Use an API Gateway service to enable caching, rate limit policies (e.g., Quota, Spike Arrest, or Concurrent Rate Limit) and deploy API resources dynamically.		
4.0	Output Security			
4.1	Ensure content validation controls for output security	Content Validation for Response: Validate the content type of returned data via Content-type header of HTTP response. It should match with the request's Accept header. Respond with 406 Not Acceptable response if it is not matched.		
4.2	Use appropriate HTTP response headers for output security	Recommended Use: • X-Content-Type-Options: Nosniff • X-Frame-Options: Deny (if there are no frames used in application) • X-Frame-Options: Sameorigin (in case frames are to be used in application) • Content-Security-Policy: default-src 'none' • Remove fingerprinting headers like *X-Powered-By*, *X-AspNet-Version*, etc. • Don't return sensitive data like credentials or security tokens in response • Return the proper status code according to the operation completed (e.g., 200 OK, 400 Bad Request, 401 Unauthorized, 405 Method Not Allowed, etc.).		
5	Data Processing Security			

5.1	Ensure Object level authorization	• User's own resource ID should be avoided. Use /me/orders instead of /user/654321/orders • Don't auto-increment IDs. Use UUID instead		
5.2	Ensure XML External Entities (XXE) prevention	• Enternal entites' misconfiguration may lead to SSRF (Server-Side Request Forgery) and billion laugh attacks. Configure the XML parser to disable external entity resolution • The XML parser should be configured to use a local static DTD and disallow any declared DTD included in the XML document		
5.3	Ensure data rate limiting	.Rate limit the data processing wherever applicable in order to avoid brute force attacks.		
5.4	Do not use test environment in production mode	Make sure your application is set to production mode before deployment. Running a debug API in production could result in performance issues & unintended operations such as test endpoints and backdoors. It may expose data sensitive to the organization or development team.		
6	Monitoring Security			
6.0	Ensure API logging & monitoring mechanism	The API logs must be stored in a centralized log management system. API monitoring includes auditing, logging, and version control for all APIs and their components. This helps in the troubleshooting process when and if a problem occurs.		
6.1	Limit number of API calls	Set a quota on the API calls count, i.e. put limitations on the number of times an API is called.		

Annexure-II: Cloud Based Checklist

Cloud Based Outsourcing Service Arrangements Cloud Service Provider's (CSP) Compliance Matrix				
Clause ID	Clause Description			
		Consent/comments by Responsible functions	Existing Controls at CSP	Remarks (If Any)
E. PERMISSIBLE CLOUD OUTSOURCING ARRANGEMENTS				
1	Please confirm whether this service/function is material or non-material as per below mentioned definition provided by SBP. 1. For the purpose of these regulations, material workload means all systems, applications, and services that are fundamental for carrying out business of an RE (Regulated Entity)/bank, and if disrupted, have the potential to significantly impact an institution's business operations, reputation or profitability.			

	2. REs may outsource their workloads to CSPs in the following manner: a) All type of workloads (i.e. material and non-material) may be outsourced to reputable onshore (i.e. domestic) CSPs; b) EMIs, non-designated PSOs/ PSPs may outsource their material and non-material workloads to offshore (i.e. outside Pakistan) CSPs; c) Banks, MFBs, DBs, DFIs and designated PSOs/PSPs may outsource their non-material workloads to offshore CSPs. However, outsourcing of their material workloads to offshore CSPs shall be subject to SBP approval whereby SBP may grant approval on case to case basis, after considering the following: i. Systemic implications of the CO (cloud outsourcing) arrangement ii. Institution specific risks iii. Legal and other strategic risks iv. Data processing and storage v. Availability and quality of services vi. Security and other controls vii. Contingency and exit planning viii. Resilience ix. Sub-contracting x. Assurance mechanism xi. Role and responsibilities d) For approval to outsource material workloads to offshore CSPs, banks, MFBs, DBs and DFIs shall submit their request to BPRD whereas designated PSOs/PSPs shall submit it to PSP&OD; e) While granting approval to banks, MFBs, DBs, DFIs and designated PSOs/PSPs, SBP may impose additional terms and conditions over and above the requirements of this framework; f) For CO arrangements, REs may use any service and deployment model as per their requirements and risk appetite; g) REs shall give preference to onshore CSPs for outsourcing their workloads; h) REs shall not process and store their data in unfriendly or hostile jurisdictions;			
	3. Outsourcing of services to CSPs does not absolve the REs from their prime responsibilities including managing and running the business operations effectively, legal and regulatory compliance, and protection of customers' data.			
	4. SBP may instruct any RE to restrict outsourcing of their workloads to CSPs due to its systemic impact, unacceptable risks and any other concerns.			
	5. REs shall submit details of their CO arrangements to SBP, as and when required.			

	6. SBP may instruct REs to shift their cloud based workloads to SBP designated onshore community cloud as and when the same is available.			
F. GOVERNANCE				
2	1. Develop a comprehensive policy for CO duly approved by their BoD. In this regard, the REs can also amend their existing 'Policy for Outsourcing Arrangements' to include/update CO. The policy shall encompass all services, as per requirements provided in section E above that can be outsourced to CSP, and at least include all those aspects that have been prescribed in this framework.			
	2. Conduct appropriate due diligence of CSPs and proactively identify any risks emanating from their CO arrangements including risks associated with sub-contracting by CSPs.			
	3. Update their Enterprise Risk Management framework or other relevant policies for effective oversight and management of risks emanating from the CO arrangement(s). The framework shall include sub-contracting risks, assessment of cloud service location(s) especially if outside Pakistan with specific focus on areas including but not limited to legal aspects; regulatory issues; jurisdictional concerns; availability; security and resilience of information assets and services; connectivity; political and security situation; ease of oversight; plausibility of RE, SBP and external audit staff to travel for onsite assessment/ audit or alternate assurance mechanism.			
	4. Delegate cloud specific governance responsibilities such as for overseeing adherence to regulatory as well as performance requirements, including cloud service SLAs, reviewing of KPIs and KRIs, incidents (including cybersecurity incidents) and other relevant matters to the ITSC. In this regard, the ToRs of ITSC shall be suitably amended to include these responsibilities			
	5. Undertake all CO arrangements through legally binding SLAs, which shall at least include the areas prescribed in Appendix – I. These SLAs must be vetted by the legal function of the RE and be executed by the REs (except branches of foreign banks) themselves instead of their parent company or subsidiary, with governing law preferably as law of Pakistan. However, compliance with the laws of Pakistan, along with compliance to any legal obligation as prescribed by the host country of the CSP, shall be mandatory at all times.			
	6. Define and agree upon the roles and responsibilities of the IT and operational departments (e.g. requirement analysis, performance testing, UAT, responsibility for data validation, etc.), before transferring information assets and services to a CSP.			

	7. Ensure that the CO arrangements are compliant with the relevant legal and regulatory requirements, and the IA functions of the REs shall provide independent certification to their BoDs in this regard.			
G. DUE DILIGENCE OF CLOUD SERVICE PROVIDER				
3	REs shall exercise reasonable care before entering into CO arrangements. To ensure effective management of the associated risks, REs shall conduct reasonable due diligence of the CSPs and their material sub-contracting arrangements by using defined criteria which shall include the following:			
	1. Evaluation of feasibility of CO arrangements including cost effectiveness, quality of service, and legal / regulatory / compliance risks.			
	2. Ability of CSP to meet legal and regulatory requirements of Pakistan.			
	3. Assessment of financial strength and resources.			
	4. Competence, business structure, experience, track record in delivering such services.			
	5. Assessment of CSPs ability to comply with necessary minimum controls including physical security / internal controls based on the intended workloads, especially with respect to confidentiality, integrity, availability and resilience.			
	6. Assessment of corporate governance and entity level controls.			
	7. Assessment of CSPs ability to provide REs the control over data residency enabling them to shift over preferred data center instance, depending upon the cloud service model, in order to host these services at such locations/countries/regions considering geopolitical risks.			
	8. Cybersecurity and IT capabilities including adherence to international standards and best practices.			
	9. Sub-contracting risk management.			
	10. Data security related controls.			

	11. Access, audit and information rights of REs, SBP and external auditors of the REs.			
	12. Support services.			
	13. Contingency, resilience and exit arrangements.			
	14. Up to date certification and attestation of the CSPs including but not limited to IT service delivery, business continuity & disaster recovery, cyber / information security, and data center Tier III certification.			
	15. Liability of claims / penalties on CSPs for: a) Unauthorized transactions; b) Service disruptions; c) Security breaches; d) Enforcement and penal actions that may be taken by regulatory and legal authorities against the REs for not complying the regulatory and legal requirements, due to faults by CSPs.			
	16. For material workloads: a) Threat & Vulnerability Assessment or equivalent independent assessments of data centers to identify the security and operational weaknesses. The scope of such assessments shall include physical and environmental security, perimeter security, access controls, security & emergency procedures, monitoring, redundancy, natural disasters, and the political and economic climate of the country in which the data center resides. The assessment shall cover all data centers where the REs' data / systems will reside; b) Independent assessments instead of solely relying on attestations by the CSPs, and the results shall be reviewed by REs' IA as well as Information Security (IS) function. However, the REs may consider SOC Reports (level 1, 2 & 3).			
H. OVERSIGHT				
4	The risk exposures and effectiveness of the corresponding controls may vary over the tenure of the CO arrangements. In this regard, REs shall:			
	1. Develop and maintain an effective oversight mechanism including but not limited to the assessment of performance against desired service levels and ongoing viability of the CSP and its services, cybersecurity practices and controls, changes in service location(s), sub- contracting, change of ownership, control environment; and timely response to emerging risks and issues.			
	2. On an ongoing basis, review and monitor the CSP's compliance with legal, regulatory and contractual obligations.			

	3. Monitor access to their cloud data/workloads, wherever possible such as through cloud activity reports.			
	4. Review internal control assessment / audit reports of the CSPs, in order to obtain assurance regarding the security and resilience.			
	5. For material workload, conduct comprehensive audit of the CSPs, either themselves or through third party assessors / pooled audits, at least once in two years. The scope of the audit shall at least include the infrastructure and related software used to deliver cloud services to the RE. However, in case where audit/onsite assessment cannot be conducted due to a valid reason(s), REs may rely on internationally recognized third party certifications and reports made available by the CSPs, after sufficient understanding and review of their scope, methodology and the ability of the assessors.			
I. CONTINGENCY PLANNING				
5	REs shall develop contingency plan for their CO workloads in order to deal with any disruption/degradation of cloud related services. The contingency plan shall take into account all possible scenarios regarding the unavailability of CSP related services due to various reasons such as technical/connectivity issues, inability of CSP to provide services due to legal actions in their respective jurisdictions, etc. In this regard, REs shall:			
	1. Prudently select appropriate implementation option (service and deployment model, availability zones, server/server-less, etc.) along with related communication technologies, to offer better resilience that commensurate with their workload.			
	2. Maximize the redundancy by design and workload distribution, and implement health and monitoring checks for ensuring HA of their cloud workloads.			
	3. Ensure redundant and robust connectivity arrangements through different international internet cables and include penalties for disruption and downtimes in their agreements.			
	4. Define clear roles and responsibilities including responsibility for signing off, updating and activating the contingency plan.			
	5. Periodically review and update the contingency plan, taking into account developments which may affect their feasibility. These may include increase in number of availability zones, changes in business requirements, new viable alternate CSPs, technological changes, etc.			

	6. Periodically (at least once annually) test the contingency plan against various scenarios including disruption of internet / communication services, unavailability of CSP, etc. Where possible, REs may conduct collaborative testing of their contingency plan with their CSPs. Further, the REs shall ensure that the deficiencies identified during testing are recorded and corrective actions are implemented.			
J. RIGHT TO AUDIT, ACCESS AND INFORMATION				
6	REs shall ensure that CO does not hinder SBP in conducting its supervisory functions. In this regard, the REs shall comply with the following requirements:			
	1. Ensure that their internal & external auditors/ independent assessors and SBP have right to conduct audits and onsite assessments of the CSP and its sub-contractors, if required. Further, there should be no restriction or prohibition on access to REs' cloud related information assets and services for the RE, its auditors, independent assessors or SBP's authorized staff or such visits are otherwise not impractical.			
	2. Ensure that access, audit and information rights provided through the contractual arrangement include where relevant: a) Premises, data, devices, information, systems, and networks used for providing the cloud services or monitoring its performance. These may include CSP's (and its sub-contractors) policies, processes, and controls; b) Results of security testing carried out by CSP or on its behalf, on its applications, data, and systems to assess the effectiveness of the implemented cybersecurity processes and controls; c) Results of security testing carried out by the sub-contractors or on its behalf, on its applications, data, and systems, where applicable, to ascertain effectiveness of the cybersecurity processes and controls; d) Company and financial information; e) CSPs' external auditors, personnel, and premises.			
	3. In case, where audit/onsite assessment cannot be conducted for a valid reason(s), REs may rely on internationally recognized third party certifications, and reports made available by the CSP. However, reliance on these third party certifications and reports shall be supported by adequate understanding and review of the scope, the methodology applied therein and the ability of the third party and CSP to clarify matters relating to the assessment. Further, the REs shall have contractual right to request for the expansion of the scope of the certifications / assessments / audits to cover relevant controls and systems.			

	4. Ensure that CSPs timely provide any information requested by SBP, whenever required.			
	5. Follow up with the CSP to ensure that all appropriate and timely remediation actions are taken to address any audit findings.			
K. EXIT PLANNING				
7	REs shall develop an exit plan by considering the materiality and impact of their workloads outsourced to CSPs. In this regard, REs shall comply with the following requirements:			
	1. Ensure that the exit plan covers scenarios for stressed and non-stressed exit circumstances.			
	2. Ensure that the exit plan has defined trigger events, alternative solutions, transition plans, and roles and responsibilities including responsibility for signing off, updating and activating the plan.			
	3. Periodically review and test the exit plan, taking into account developments which may affect its feasibility.			
	4. Implement measures including but not limited to contractual or escrow arrangements, to ensure continuity of critical business services in case of exit.			
	5. Ensure complete removal of data including logs from all locations of CSP in case of exit.			
	6. To avoid the lock-in and dependency risks, REs shall in their CO arrangement contracts: a) Avoid inclusion of any lock-in clause or exclusivity arrangements; b) Ensure that they have right to terminate the CO agreement at least in the following circumstances: i. Change in ownership of the CSP ii. Insolvency or liquidation of the CSP iii. CSP goes into judicial administration iv. CSP is in breach of applicable laws, regulations or contractual provisions v. Significant and material breach of security or confidentiality vi. Demonstrable deterioration to perform the contracted service c) Ensure that the minimum termination period is documented in their CO contracts.			
L. SUB-CONTRACTING				

8	The CO arrangements expose REs to various risks relating to sub-contracting due to improper/non implementation of controls by the sub-contractors. For material sub-contracting, the REs shall comply with the following requirements:			
	1. Have visibility of the CSP supply chain by ensuring that the CSP maintains and provides an updated list of its sub-contractors.			
	2. Consider potential impact of large, complex sub-contracting by the CSPs on their operational resilience, and ability to oversee and monitor the emanating risks.			
	3. Only permit sub-contracting by CSPs if such arrangements do not give rise to excessive operational risks, and sub-contractor agrees to comply with all applicable legal, regulatory, contractual, audit and access requirements including granting REs and SBP contractual access, audit and information rights.			
	4. Review material sub-contracting agreements of the CSP and ascertain that the legal, regulatory, operational, and cybersecurity requirements are complied with, throughout the supply chain.			
	5. Ensure that the CSPs have the capability and capacity to oversee any material sub- contracting on an ongoing basis.			
M. USER ACCESS MANAGEMENT AND AUTHENTICATION				
	REs shall implement complete life cycle of user access management for their cloud related workloads, while complying with the following requirements:			
	1. Implement at-least four eye principle for user access administration.			
	2. Periodically review user access right changes independently.			
	3. Ensure that the use and access of service, generic and administrative accounts are controlled and monitored. Moreover, the REs shall implement MFA and limit use of these accounts through dedicated machines only.			
	4. Create separate account of administrative users for routine operations, and implement enhanced password controls (length, complexity, age).			
	5. Implement MFA and IP source restrictions (wherever possible) for their users accessing cloud environment.			
	6. Monitor and document the use of master account, and permit its usage only under exceptional circumstances.			

	7. Implement access controls for data backups including log data, of cloud related workloads.			
	8. Ensure that CSPs do not have access to REs' systems, software and data.			
N. CHANGE AND CONFIGURATION MANAGEMENT				
	REs shall plan and implement configuration management in conjunction with IT change management to ensure safe and secure operations of cloud services. In this regard, REs shall comply with the following requirements for their cloud related workloads:			
	1. Implement mechanism for detecting unauthorized changes to cloud environment, and configure automated alerts for the changes.			
	2. Ensure CM procedures for cloud related workloads are documented and mutually agreed with the CSP. These shall at least include change request and approval procedures, change prioritization and impact assessment, change reporting, roles and responsibilities, timeframe for patching and software releases.			
	3. Ensure that the CSPs have well-defined and robust CM controls, and notify the REs in advance of the changes.			
	4. Ensure that the changes are tested before their implementation on the production environment.			
	5. Define roles and responsibilities of REs staff for configuration management of the cloud environment, and at least segregate infrastructure, security and application roles.			
	6. Create and maintain baselines for cloud hosted systems, and periodically review, monitor, report and remediate non-compliance with the baselines.			
O. INCIDENT MANAGEMENT				
9	Effective and efficient remediation of the incidents requires timely detection and proper integration with the incident response and management processes. With the increase in sophistication of cyber-attacks, there is a need to use advance analytics to correlate events across multiple systems. For incident management, REs shall comply with the following requirements for their cloud related workloads:			

	1. Define and document criteria, performance requirements and procedures for escalation, notification, containment and closure of incidents (including IT, cyber incidents) in consensus with the CSP(s).			
	2. Ensure access to incident and root cause analysis reports of the CSPs.			
	3. Designate a SIRT to provide timely response to IT/cyber incidents. In this regard, roles and responsibilities of CSP and REs' teams shall be formalized.			
	4. Ensure that CSPs shall provide reasonable access to necessary information to assist in any REs' investigation arising due to an incident in the cloud.			
	5. Ensure that the CSPs conduct formal post incident review of the material cloud related incidents and provide their report to the RE.			
	6. Ensure that ITSC as part of their oversight reviews and discusses cloud related incidents.			
	7. Periodically review and test Incident Response Plan of cloud related workloads at least once annually, keeping in view cybersecurity as one of key considerations.			
P. DATA SECURITY				
10	Outsourcing of the workloads to the CSPs does not relieve the REs from the responsibility of safeguarding data confidentiality and integrity. In this regard, REs shall:			
	1. Encrypt data at rest (including backups) and in transit using strong and non-obsolete cryptographic algorithms.			
	2. Desensitize the production data before porting or using it on non-production environment(s).			
	3. Ensure that their data in the cloud environment is clearly identifiable and segregated.			
	4. Take appropriate measures for the protection of Personally Identifiable Information (PII); and ensure compliance with the requirements of laws of Pakistan at all times. Further, REs shall ensure that CSPs do not disclose their data to any third party including foreign governments / courts / law enforcement agencies without their consent.			
	5. Ensure that CSP does not use their data for any commercial purposes.			

	6. Implement reasonable backup and restoration testing mechanism, depending on the nature of the workloads in compliance with the defined RPOs. Further, the backup mechanism shall have ransomware protection, and the backup restoration testing exercise shall be conducted at least on a half-yearly basis.			
	7. Classify information assets in terms of their sensitivity, confidentiality & availability, and implement additional controls for high value cloud information assets.			
	8. Implement controls to prevent unauthorized exfiltration of data from the cloud environment. These controls shall include deployment of content inspection technologies, controls on data downloading and extraction, monitoring unusual data access, etc.			
	9. Ensure that they are notified about any proposed change in the location of their data, and have contractual right to reject such change, or terminate the CO arrangement on such grounds.			
	10. Ensure that data is deleted from all storage locations of the CSP following an exit or termination of the CO arrangement, and where applicable, from the systems of any sub- contractor by requesting written confirmation from the CSP.			
Q. CRYPTOGRAPHIC KEY MANAGEMENT				
11	CSPs use cryptographic controls to secure access and segregate customers' data. Hence, the security of the cryptographic keys is critical for ensuring the data security. CSPs offer a variety of key management options/features, which can be selected by the REs for implementation based on the significance of their workloads. In this regard, the REs shall comply with the following requirements:			
	1. Develop and implement policies and procedures governing the lifecycle of the cryptographic material.			
	2. Ensure that details of the cryptographic algorithms and other related parameters such as key lengths, renewals etc. are reviewed by a subject matter expert.			
	3. Ensure that details of the location, ownership and management of the encryption keys and HSM are agreed with the CSP and documented.			
	4. Ensure that the cryptographic keys are unique and generated only by the REs. Further, REs must have the sole ability to administer/manage these keys and HSM.			
	5. Periodically change the cryptographic keys in accordance with the international standards and best practices			

	6. Ensure that the encryption keys are stored separate from the virtual images and information assets.			
	7. For material workloads, deploy/implement HSM with due controls.			
R. TOKENIZATION				
12	Depending on the sensitivity of data workload, REs may implement tokenization to minimize the data footprint. While implementing tokenization, REs shall assess and evaluate the features and data interactions of the tokenization solution. REs shall also ensure that the CSPs do not have access or control over the tokenization solution.			
S. NETWORK ARCHITECTURE				
	The network structure and logical layout is of paramount importance in any cloud implementation. Therefore, the REs must implement controls for protection against plausible threats/attacks including cloud specific attacks, by implementing the following requirements:			
	1. Ensure security of their CO arrangements and on premise environments by implementing controls at appropriate locations to detect and mitigate security breaches and ongoing attacks. These controls shall include but not limited to perimeter security, network IDS/IPS, WAF, DDoS protection, etc.			
	2. Implement network segmentation based on type of workloads (e.g. production, pre- production, quality assurance, development, etc.) and purpose (e.g. end-users, critical servers, other servers, middleware, interface, etc.). In this regard, a dedicated network segment (i.e. management network) not accessible from other operational segments shall be implemented for administration purposes. Further, all internet traffic shall be routed through a dedicated network segment (i.e. security segment) and other network segments shall not have direct internet access.			
	3. Secure traffic between the cloud and on premise environment using a VPN or direct network connection with stringent access control rules configured to ensure routing of traffic from/to dedicated source and destination IPs.			
	4. Monitor and control access to and security of the cloud environments. In this regard, regularly review the firewall rules and access lists, especially after any changes.			
T. SECURITY TESTING				

13	The dynamic and evolving nature of cyber threats requires a high degree of validation and testing of security posture of an enterprise, on periodic basis. However, security testing of the systems and applications in the cloud environment is challenging due to the inherent shared service model. In this regard, REs shall comply with the following requirements:			
	1. Conduct vulnerability assessment, penetration testing and scenario based security testing of their systems hosted with the CSPs on periodic basis, at least once annually.			
	2. Ensure that CSPs conduct vulnerability assessment and penetration testing for the infrastructure and applications managed by them, at least once annually in order to provide security assurance to the REs. Further, the REs shall be fully cognizant of the scope of such assessments while examining the results.			
	3. Ensure that security testing is conducted while taking into consideration various scenarios and threats that are unique to cloud services including but not limited to hypervisor jumping, weak application programming interfaces, DoS hyper jacking, wrapping attacks, cloud malware injection, side channel attacks, etc.			
	4. Ensure that all vulnerabilities identified for their cloud related workloads are categorized in terms of risk, tracked and rectified (including post validated). For the infrastructure and applications managed by the CSPs, REs shall implement alternate mechanism for obtaining assurance that the vulnerabilities are timely rectified.			
	5. In case of material CO, ensure independent Threat & Vulnerability Assessment of CSP's data centers hosting the data/systems of REs, at least once annually.			
U. SECURITY EVENT MONITORING				
14	REs shall establish mechanisms for SEM by complying with the following requirements:			
	1. Wherever possible, leverage the controls/tools available in the cloud environment to enforce consistent security standards and baselines, automated response, remediation and notification.			
	2. Integrate CSP related services with their SIEM solutions to provide a detailed analysis of the security logs. In this regard, cloud specific incident scenarios with correlation rules shall be implemented. Further, AI and ML driven technologies may be explored and preferably adopted, where available.			
	3. Ensure that cloud related activities are effectively monitored by their SOC on 24x7 basis.			
V. OTHER REQUIREMENTS				

15	1. REs shall monitor and review capacity utilization of their cloud workloads.			
	2. REs shall provide adequate training of the cloud environment, to their end-users and privileged users.			
	3. All security incidents / breaches shall be reported to SBP in compliance with the requirements specified in the 'Enterprise Technology Governance & Risk Management Framework for Financial Institutions' or as advised by SBP from time to time. Further, REs shall conduct investigations to identify the root cause, take appropriate actions to prevent recurrence of such incidents in future and fix responsibility for such lapse.			
	4. For material workloads, REs shall provide following information to SBP1 one month before placing their services with the CSPs: a) Name of the CSPs, and their parent company (if any); b) Description of the activities and details of data to be placed with the CSP; c) Date of commencement / renewal / expiry of services; d) Last contract renewal date (where applicable); e) Service and Deployment Models.			

Past Experience / Contracts

Contracts over *[insert amount]* during the last three years:				
Procuring Agency	Value	Year	Goods/Services Supplied	Country of Destination

Historical Contract Non-Performance, and Pending Litigation and Litigation History

[The following table shall be filled in for the Applicant and for each member of a Joint Venture]

Applicant's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member Name: *[insert full name]*
IFP No. and title: *[insert IFP number and title]*
Page *[insert page number]* of *[insert total number]* pages

☐ Not debarred due to deviation from commitment of Bid Securing Declaration-☐ Not debarred due to non-performance			
Year	**Non-performed portion of contract**	**Contract Identification**	**Total Contract Amount (current value, currency, exchange rate and PKR equivalent)**
[insert year]	*[insert amount and percentage]*	Contract Identification: *[indicate complete contract name/ number, and any other identification]* Name of Procuring Agency: *[insert full name]* Address of Procuring Agency: *[insert street/city/country]* Reason(s) for nonperformance: *[indicate main reason(s)]*	*[insert amount]*
Pending Litigation, in accordance with Section III, Qualification Criteria and Requirements			
☐ Pending litigation in accordance with Section III, Qualification Criteria and Requirements, Sub-Factor 2.3 as indicated below.			

Year of dispute	**Amount in dispute (currency)**	**Contract Identification**	**Total Contract Amount (currency), ~~US$~~ PKR Equivalent (exchange rate)**

[insert year]	*[insert amount]*	Contract Identification: [indicate complete contract name, number, and any other identification] Name of Procuring Agency: *[insert full name]* Address of Procuring Agency: *[insert street/city/country]* Matter in dispute: *[indicate main issues in dispute]* Party who initiated the dispute: *[indicate "Procuring Agency" or "Supplier"]* Status of dispute: *[Indicate if it is being treated by the Adjudicator, under Arbitration or being dealt with by the Judiciary]*	*[insert amount]*

☐ No consistent history of court/arbitral award decisions in accordance with Section III, Qualification Criteria and Requirements, Sub-Factor 2.4.

☐ Consistent history of court/arbitral award decisions in accordance with Section III, Qualification Criteria and Requirements, Sub-Factor 2.4 as indicated below.

Year of award	**Outcome as percentage of Net Worth**	**Contract Identification**	**Total Contract Amount (currency), PKR Equivalent (exchange rate)**
[insert year]	*[insert percentage]*	Contract Identification: [indicate complete contract name, number, and any other identification] Name of Procuring Agency: *[insert full name]* Address of Procuring Agency: *[insert street/city/country]* Matter in dispute: *[indicate main issues in dispute]* Party who initiated the dispute: *[indicate "Procuring Agency" or "Supplier"]* Court/ arbitral award decision: *[Indicate if the award decision was against the Applicant or any member of a joint venture.]y]*	*[insert amount]*

Current Contract Commitments / Works in Progress

Bidders and each member to a JV should provide information on their current commitments on all contracts that have been awarded, or for which a letter of intent or acceptance has been received, or for contracts approaching completion, but for which an unqualified, full completion certificate has yet to be issued.

Current Contract Commitments					
No.	Name of Contract	**Employer's Contact Address, Tel, Fax**	**Value of Outstanding Work [Current Eq. PKR]**	**Estimated Completion Date**	**Average Monthly Invoicing Over Last Six Months [Eq. PKR/month)]**
1					
2					
3					
4					
5					

Financial Situation and Performance

[The following table shall be filled in for the Applicant and for each member of a Joint Venture]

Applicant's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member Name: *[insert full name]*
IFP No. and title: *[insert IFP number and title]*
Page *[insert page number]* of *[insert total number]* pages

1. Financial data

Type of Financial information in (currency)	**Historic information for previous _[insert number] years, [insert in words] (amount in currency, currency, exchange rate*, PKR equivalent)**				
	Year 1	Year 2	Year 3		
Statement of Financial Position (Information from Balance Sheet)					
Total Assets (TA)					
Total Liabilities (TL)					
Total Equity/Net Worth (NW)					
Current Assets (CA)					
Current Liabilities (CL)					
Working Capital (WC)					
Information from Income Statement					
Total Revenue (TR)					
Profits Before Taxes (PBT)					
Cash Flow Information					
Cash Flow from Operating Activities					

* Refer ITA 14 for the exchange rate

3. Financial documents

The Applicant and in case of JV, members of JV shall provide copies of financial statements for *[number]* years pursuant Section III, Qualifications Criteria and Requirements. The financial statements shall:

(a) reflect the financial situation of the Applicant or in case of JV member, and not an affiliated entity (such as parent company or group member).

(b) be independently audited or certified in accordance with local legislation.

(c) be complete, including all notes to the financial statements.

(d) correspond to accounting periods already completed and audited.

☐ Attached are copies of financial statements[1] for the *[number]* years required above; and complying with the requirements.

[1] If the most recent set of financial statements is for a period earlier than 12 months from the date of Application, the reason for this should be justified.

Average Annual Turnover (Annual Sales Value)

[The following table shall be filled in for the Applicant and for each member of a Joint Venture]

Applicant's Name: *[insert full name]*
Date: *[insert day, month, year]*
Joint Venture Member Name: *[insert full name]*
IFP No. and title: *[insert IFP number and title]*
Page *[insert page number]* of *[insert total number]* pages

Annual Turnover Data			
Year	**Amount** **Currency**	**Exchange rate*** **(If applicable)**	**PKR equivalent**
[indicate calendar year]	*[insert amount and indicate currency]*		
		Average Annual Turnover **	

* Refer ITA for date and source of exchange rate.

** Total PKR equivalent for all years divided by the total number of years. See Section III, Qualification Criteria and Requirements, ITA.