STANDARD BIDDING DOCUMENTS

Request for Proposal

Tender for Loan Origination System (LOS)

(Single Stage: Two Envelope Procedures)

NBP

Head Office
NBP Building, I.I. Chundrigar Road
Karachi. Pakistan.
Phone No. +92 -21- 99220100

Contents

1. Invitation to e-BID (Section-I)

PROCUREMENT OF LOAN ORIGINATION SYSTEM

1. National Bank of Pakistan, one of the largest commercial banks operating in Pakistan invites electronic bids from the original manufacturers or service providers, etc., registered with the Income Tax, Revenue Board, and Sales Tax Department for the supply of the Loan Origination System.
2. Bidding document as per regulations, containing eligibility/qualification criteria and requirements, detailed terms and conditions, is available free of cost on PRRA's E-PAK Acquisition and Disposal System (EPADS) at https://eprocure.gov.pk and www.nbp.com.pk.
3. The electronic bids must be submitted by using EPADS on or before 17th June 2025, at 03:00 pm. Manual bids submission shall not be accepted. Electronic bids will be opened on the same day at 03:30 pm.

Note:

a) NBP reserves the right to cancel this invitation at any stage prior to the announcement of tender results as per PPRA rules. This advertisement is also available on the NBP **(www.nbp.com.pk)** and PPRA **(www.ppra.org.pk)** websites.
b) The notification of the GRC constituted in terms of Rule-48 of PPRA rules, 2004 is provided on EPADS at www.eprocure.gov.pk and on PA's website https://www.nbp.com.pk
c) Original Bid Security instrument MUST BE submitted to the undersigned office on or before the online submission deadline of the bid.
d) In case of any technical difficulty in using EPADS, prospective bidders may contact the PPRA Team, director MIS Room No. 109, 1st Floor, FBC building sector G-5/2, Islamabad. Contact number 051-111-137-237.

(Divisional Head)
Procurement Division,
Logistics, Communications & Marketing Group,
National Bank of Pakistan
3rd Floor, Head Office Building, Karachi.
021-99220331, 021-38902435

Brief Description of the RFP

The National Bank of Pakistan (NBP) invites proposals for an on-premises Loan Origination System (LOS) platform. This platform should automate loan origination processes, manage workflows and decision-making, integrate seamlessly with NBP's existing applications, and offer robust functionality, user-friendliness, security, and scalability. NBP seeks a reliable partner to deliver a solution that aligns with its digital transformation goals and enhances customer experience. The selection process will follow a single-stage, two-envelope, open competitive procedure. Proposals should include detailed plans for development, implementation, integration, customization, support, and maintenance. The successful bidder will be responsible for delivering a solution that meets NBP's current and future needs. The RFP is also available at www.ppra.or.pk under the procurement section.

Organizational Overview

NBP, a leading financial institution established in 1959, is committed to setting industry standards through optimized processes and technology. With a vast network of over 1500+ branches worldwide, NBP provides a comprehensive range of banking services.

To further enhance its digital capabilities, NBP seeks a state-of-the-art, on-premises Loan Origination System (LOS) platform. This platform should seamlessly integrate with NBP's core banking, mobile banking, and other systems, delivering a centralized and efficient solution for loan origination.

System Scope

The scope of works in the Request for Proposal (RFP) for the LOS would include but not be limited to providing service/solution for digital loan origination (Conventional and Islamic) and its maintenance and support for the tenure of the Contract.

S. No	Requirement
1.	Loan Origination (Retail/Consumer, Corporate, Commercial, SME, FI & Agri), Monitoring System (Admin module included).
2.	The platform should be capable of integration with various internal systems like CBA, eDMS, NADRA (BVS-Verisys), eCIB (direct or indirect), Tasdeeq, NBP Website, DataCheck, AML/Fraud System, Middleware (ESB/SOA), SafeWatch, Internal Blacklist, Anti Money Laundry, Multifactor Authentication Server, SMS Gateway/Middleware, 1Link, Email Exchange Server, Document Scanning (OCR capability would be required fast and secure scanning and uploading of documents), HRMS, 3rd party applications, Treasury, GL Application and other platforms supported by the Regulator/Industry, and auxiliary applications (Social Media, Credit Rating Agencies) but not limited to.

3.	• Farm Data Management: Detailed farm profiling, including size, location, crops, livestock, equipment, and practices. • Environmental Data Integration: Access to weather/climate data to assess impact on farm productivity. • Financial Assessment Tools: Land valuation features and integration with subsidy/grant systems. • Market Data Integration: Access to crop/livestock pricing for loan assessment. • Operational Tracking: Monitoring of seasonal cycles for cash flow analysis. • Risk Management: Fraud detection tools.

To ensure future-proofing and scalability, the LOS should be designed with a flexible architecture that can accommodate growth and technological advancements. This includes seamless integration with back-office systems and external services through APIs and microservices, as well as incorporating a built-in workflow manager, robust alerting, and comprehensive reporting capabilities.

Delivery Module

NBP seeks to procure an on-premises Loan Origination System. The system must offer comprehensive loan origination functionalities, including application processing, document management, credit decisions, and integration capabilities. Performance requirements include scalability to accommodate increasing loan volumes and adherence to stringent security standards, encompassing data encryption, access controls, and compliance with banking regulations. Seamless integration with existing bank systems, a user-friendly interface, and robust vendor support are critical considerations for this procurement.

On-Premises Model

- On-Premises Deployment: The system will be deployed on NBP's infrastructure, providing full control over hardware and software.
- API-driven Integration: Utilize well-defined APIs to integrate with existing core banking systems and third-party services.
- Vendor Support: The vendor will provide comprehensive support services, including installation, configuration, maintenance, and troubleshooting.

Security and Compliance

- Security Assessment Services (Internal): The vendor should perform assessment & testing services of the infrastructure hosting NBP services.
- Vulnerability & Penetration Testing Services (External - when requested by NBP): Vulnerability Assessment & Penetration Testing.
- Data Privacy and Security: The vendor must adhere to strict data privacy and security standards, including data encryption, access controls, and regular security audits.

- Regulatory Compliance: The solution must comply with all relevant banking regulations and industry standards.

Additional Considerations

- Disaster Recovery: The vendor should provide a comprehensive disaster recovery plan to ensure business continuity.
- Performance and Scalability: The system should be designed to handle increasing workloads and evolving business needs.
- User Experience: The system should provide a user-friendly interface that is easy to navigate and use.

Capable Platform Required to Meet Upcoming Business Needs

The LOS platform should be highly flexible, extensible, and scalable. It should integrate seamlessly with various systems, support omnichannel capabilities, and offer a user-friendly interface. Robust database optimization and connection pooling are crucial for optimal performance. The vendor must ensure compliance with all regulatory requirements and provide necessary updates and enhancements without additional cost throughout the contractual period. The platform should be able to handle a diverse range of loan products, including corporate, retail, commercial, SME, and agricultural loans.

2. Instructions to Bidders - ITB (Section-II)

Capitalized terms used in the Bid Data Sheet (BDS) and the Instructions to Bidders (ITB), unless specifically defined otherwise, shall have the same meaning as set out in the General Conditions of Contract (GCC) and the Special Conditions of Contract (SCC).

A. General

1	Scope of Bid	1.1 National Bank of Pakistan, referred to as "NBP" or "Procuring Agency" or "Bank" in these bidding documents, invites bids for LOS - Request for Proposal Bill of Payment Terms & Conditions / Quantity are attached as Section- IX & X.
		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 National Bank of Pakistan/Local
3	Fraud and Corruption	3.1 A Bidder may be a natural person, 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. 3.2 (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). 3.3 A 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 information 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.4 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 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 Bidders	4.1 A Bidder may be natural person, 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.

4.2 (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).

4.3 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.

4.4 Verifiable copy of the agreement that forms a joint venture, consortium or association shall be required to be submitted as part of the Bid.

4.5 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.

4.6 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.

4.7 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.

4.8 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 information 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.

4.9 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. 4.10 Bidders shall provide the Procuring Agency evidence of their eligibility, proof of compliance with the necessary legal requirements to carry out the contract effectively. 4.11 Bidders shall provide such evidence of their continued eligibility to the satisfaction of the Procuring Agency, as the Procuring Agency shall reasonably request. 4.12 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.
5	Eligible Goods and Services	5.1 All Goods and related Services to be supplied under the Contract Agreement shall have their origin in eligible source countries. 5.2 For purposes of this clause, "origin" means the place where the goods are mined, grown, or produced, or the place from which the related Services are supplied. Goods are produced when, through manufacturing, processing, or substantial and major assembly of components, a commercially recognized product results that are substantially different in basic characteristics or purpose or utility from its components. 5.3 The origin of Goods and Services is distinct from the nationality of a bidder.
6	Qualification of the Bidder	6.1 By submission of documentary evidence in its bid, the bidder must establish to NBP's satisfaction that: a) It has the financial, technical, and production/servicing capability necessary to undertake and successfully conclude the contract, meet the qualification criteria specified in the BDS, and have a successful performance history. If a pre-qualification process has been undertaken for the contract(s) for which these bidding documents have been issued, the bidder shall, as part of its bid, update any information submitted with its pre-qualification application. To establish a bidder's qualifications, and unless stated to the contrary in the BDS, the experience and/or resources of any subcontractor will not contribute to the bidder's qualifications; only those of a joint venture partner will be considered. b) in the case of a bidder, for a specific project, offering to supply key goods and components that it does not manufacture or otherwise produce itself, the bidder shall provide written evidence of due authorization by the manufacturer or producer authorizing the bidder to supply those components in Pakistan, as identified in the BDS under the Contract Agreement. This will be accomplished by submission of Manufacturer's Authorization Forms, as indicated in the section entitled Sample Forms; and

c) in the case of a bidder not undertaking business within Pakistan, the bidder is or will be (if awarded the contract) represented by an agent in Pakistan who is equipped and able to carry out maintenance, technical support, training, and repair obligations prescribed in the GCC and SCC, and/or Technical Requirements, on behalf of the bidder.

6.2 Bids submitted by a joint venture of two or more bidders/companies /partnership firms as partners shall also comply with the following requirements:

a) the bid shall be duly signed by all the collaborating partners forming a joint venture to be legally binding on all partners;

b) one of the partners shall be nominated as being in charge, and this nomination shall be evidenced by submitting a power of attorney signed by legally authorized signatories of all the partners;

c) the partner in charge shall be authorized to incur liabilities and receive instructions for and on behalf of any and all partners of the joint venture, and the entire execution of the Contract undertaken with the partner in charge;

d) the partner or combination of partners responsible for a specific component(s) of the specific project must meet the relevant minimum qualification criteria for that component;

e) a bidder/partnership firm/company may submit bids either as a single bidder on its/his/her own or as a partner in a joint venture. Furthermore, a bidder/partnership firm/company that is a bidder, whether as a single bidder or as a partner in a joint venture, cannot be a subcontractor in other bids, except for the supply of commercially available hardware or software manufactured or produced by the bidder/partnership firm/company, as well as purely incidental services such as installation/configuration, routine training, and ongoing maintenance/support. If the BDS for ITB clause 6.1 (a) allows the qualification of subcontractors nominated for certain components to be taken into account in assessing the bidder's overall qualifications, any subcontractor so nominated by any bidder is automatically disqualified from being a bidder itself or a partner in a joint venture. Non- compliance may result in the rejection of all bids in which the culprit bidder/partnership firm/company participates as a bidder or as a partner in a joint venture. As long as a bidder/partnership firm/company is in compliance with these provisions or is unaffected by them for not participating as a bidder or as a partner in a joint venture, it may be proposed as a subcontractor in any number of bids. If the BDS for ITB clause 28.1 permits the submission of bids for sub-systems or slices, then the provisions of this clause 6.2 (e) apply only to bids for the same sub-system(s), or slice(s);

f) all partners of the joint venture shall be liable jointly and severally for the execution of the contract in accordance with the contract terms, and a statement to this effect shall be included in the authorization mentioned under ITB clause 6.2 (b) above, in the bid and the Contract Agreement (in case of a successful bid).

6.3 If a bidder intends to subcontract major items of supply or services, it shall include in the bid details the name and nationality of the proposed Subcontractor, including Suppliers for each of those items. The bidder shall be responsible for ensuring that the proposed Subcontractor(s) complies with the requirements of ITB clause 4 and that any Goods or Services components of the concerned project to be provided

		by the Subcontractor comply with the requirements of ITB clause 5 and the related evidence required by ITB clause 13.1 (f) (ii) is submitted. Bidders are free to list more than one Subcontractor against each item. Quoted rates and prices will be deemed to apply to whichever Subcontractor is appointed by the bidder and any adjustment of the rates or prices shall not be permitted. NBP reserves the right to delete any proposed Subcontractor from the list provided by the bidder. Subsequent additions and deletions from the list of approved Subcontractors shall be performed in accordance with GCC clause 20 (as revised in the SCC, if applicable). For the purposes of these Bidding Documents, a Subcontractor is any supplier or service provider with whom the bidder contracts for the supply or execution of any part of the specific project to be provided by the bidder under the Contract Agreement (such as the supply of major hardware, Software, or other components of the required information technologies specified, or the performance of related Services, e.g., software development, transportation, installation, customization, integration, commissioning, training, technical support, maintenance, repair, etc.).
7	One Bid per Bidder	7.1 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. 7.2 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. 7.3 A person or a firm cannot be a sub-contractor with more than one bidder in the same bidding process.
8	Cost of Bidding	8.1 The bidder shall bear all costs associated with the preparation and submission of its bid, and NBP shall not be responsible or liable for those costs under any circumstances.
9	Site Visit	9.1 The bidder may wish to visit and examine the site or sites of the concerned project and obtain for itself, at its responsibility and risk, all information that may be necessary for preparing the bid and entering into the Contract Agreement. The costs of visiting the site or sites (all over Pakistan) shall be at the bidder's own expense. 9.2 NBP will arrange for the bidder, its personnel, or agents to access the relevant site or sites, provided that the bidder notifies NBP about a proposed visit at least fourteen (14) Days before the same. 9.3 No site visits shall be arranged or scheduled after the deadline for the submission of the bids and before the award of the contract.
10	Eligible Information Systems	10.1 For the purposes of these Bidding Documents, the Information System means all: a) the required information 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 Information System to be provided by the selected Bidder and as specified in the Contract. 10.2 All Information 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 information systems. For the purpose of this Bid, ineligible countries are stated in the section-4

		titled as "Eligible Countries". 10.3 For purposes of this Clause, "origin" means the place where the goods and services making Information System are produced in or supplied from. An Information 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. 10.4 The nationality of the supplier that supplies and install the Information System shall not determine the origin of the goods. 10.5 To establish the eligibility of the Goods and Services making Information System, Bidders shall fill the country-of-origin declarations included in the Form of Bid. 10.6 If so, required in the BDS, the Bidder shall demonstrate that it has been duly authorized for the supply and installation of Information System in Pakistan (or in respective country in case of procurement by the Pakistani Missions abroad), the Information System indicated in its Bid.

B. The Bidding Documents

<table>
<tr><td rowspan="14">9</td><td rowspan="14">Content of Bidding Documents</td><td colspan="2">9.1 The bidding documents are listed below and should be read in conjunction with Sections attached and any addenda issued in accordance with ITB clause 11.</td></tr>
<tr><td>Section-I</td><td>Brief Description of RFP</td></tr>
<tr><td>Section-II</td><td>Instructions to Bidders (ITB)</td></tr>
<tr><td>Section-III</td><td>Bid Data Sheet (BDS)</td></tr>
<tr><td>Section-IV</td><td>Eligible Countries</td></tr>
<tr><td>Section-V</td><td>General Conditions of Contract (GCC)</td></tr>
<tr><td>Section-VI</td><td>Special Conditions of Contract (SCC)</td></tr>
<tr><td>Section-VII</td><td>Technical Requirements</td></tr>
<tr><td>Section-VIII</td><td>Technical Evaluation Criteria</td></tr>
<tr><td>Section-IX</td><td>Payment Terms & Conditions</td></tr>
<tr><td>Section-X</td><td>Bill of Quantity</td></tr>
<tr><td>Section-XI</td><td>Delivery Schedule</td></tr>
<tr><td>Section-XII</td><td>Sample Forms</td></tr>
<tr><td colspan="2">9.2 Bidders are expected to examine all instructions, forms, terms, specifications, and other information in the Bidding Document and attached Sections. Failure to furnish all information required by the Bidding Documents or to submit a bid not substantially responsive to the Bidding Documents in every respect will be at the bidder's risk and may result in the rejection of the bid.</td></tr>
<tr><td>10</td><td>Clarification of Bidding Documents and Pre-bid Meetings</td><td colspan="2">10.1 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.
10.2 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.
10.3 Copies of the Procuring Agency's response will be forwarded to all identified</td></tr>
</table>

		Prospective Bidders through an identified source of communication, including a description of the inquiry, but without identifying its source. 10.4 In case of downloading of the Bidding Documents from the website of PA, the response to all such queries will also be available on the same link available at the website. 10.5 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. 10.6 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. 10.7 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. 10.8 The Bidder may wish to visit and examine the site or sites of the Information 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. 10.9 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. 10.10 No site visits shall be arranged or scheduled after the deadline for the submission of the Bids and prior to the award of Contract.
11	Amendment of Bidding Documents	11.1 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. 11.2 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: 11.3 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. 11.4 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.

C. Preparation of Bids

12	Language of Bid	12.1 The bid prepared by the bidder and all correspondence and documents related to the bid exchanged by the bidder and NBP shall be written in the language specified in the BDS. Any printed literature furnished by the bidder as part of its bid may be written in another language, as long as such literature is accompanied by a translation in the language specified in the BDS, in which case, for the purpose of interpretation of the bid, the translation shall govern.
13	Documents Comprising the Bid	13.1 The bid submitted by the bidder shall comprise of: a) Technical proposals are to be submitted separately in the relevant EPADS section. Technical proposal will consist of the bidder's complete profile, complete technical offer, compliance sheet in the given format, relevant technical brochures; key highlights of the product/Solution offered, and allied details. Required information in the technical proposal is mentioned in Section-I, II, III, IV, V, VI, VII, X, and XI and any other attachments/documentary evidence. b) A Bid Form duly completed and signed by a person, or persons duly authorized to bind the bidder to the Contract Agreement. c) The financial proposal will consist of BOQ Section-X, Payment Terms & Conditions Section-IX and Bid Security Payment Order sealed all price schedules duly completed in accordance with ITB clauses 14, 15, and 18 and be signed by a person or persons duly authorized to bind the bidder to the Contract Agreement. Financial proposals of bidders whose technical proposals are found to be substantially responsive, technically qualified, and compliant with the given specifications and allied requirements will be opened on an announced date. d) Bid security is furnished in accordance with ITB clause 17. It must be attached as a scanned copy on the EPADS. e) In case the bidder is a company, a resolution of the board of directors passed in accordance with the articles of association of the company authorizing specific officers to sign on behalf of the bidder; in case the bidder is a partnership firm, a partners resolution passed in accordance with the partnership deed authorizing a partner or partners to sign on behalf of the bidder; in case the bidder is a sole proprietorship, a declaration of sole proprietorship and confirmation that the sole proprietor shall sign as the bidder; and in case the bidders have formed a joint venture, then a letter confirming the formation of the joint venture and authorizing the lead bidder's representative to sign on behalf of the bidders in the joint venture. The above resolutions/letters/declarations should authorize the signatory of the bid to commit the bidder, in accordance with ITB clause 19.2; f) Attachments: i) The bidder's qualifications should be set out as per the attached criterion mentioned in Section-I: Mandatory Requirements for Bidders and Supplier's Eligibility/ Selection Criteria. (ii) Documentary evidence

		establishing NBP's satisfaction, and in accordance with ITB clause 6, that the bidder is qualified to perform the contract if its bid is accepted. In case of pre- qualification of bidders having been undertaken, and in pursuance of ITB clause 6.1 (a), the bidder must provide evidence on any changes in the information submitted as the basis for pre-qualification or if there has been no change at all in the said information, a statement to this effect; ii) Relevant business and service partnership certificates and manufacturer's authorizations specified as required in the BDS for ITB Clause 6.1 (b);
14	Bid Prices	14.1 The prices of services/goods and components of a system shall be clearly and individually specified a) Services/Goods supplied from outside the country where NBP is based: Unless otherwise specified in the BDS, the prices shall be quoted on a DDP basis with delivery at NBP Head Office Karachi and shall be inclusive of all taxes, stamp duty, duties, levies, sales or other similar tax and fees imposed in the country where NBP is based. 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. b) Locally supplied Services/Goods: Unit prices of Services/Goods offered from within the country where NBP is based shall be quoted on a FOR basis and shall be inclusive of all duties, levies, fees, stamp duties, taxes, sales, and other similar taxes incurred until delivery of the Services/Goods. Insurance charges shall be for the account of the bidder c) Additional charges: All inland transportation charges (If any) must be included in prices quoted for goods referred to in Clause 14(a) and (b) above. Any additional costs of any support, service level agreement, or license cost as required must also be quoted separately along with its justification and rationale.
15	Bid Currencies and Prices	15.1 Unless otherwise specified in the BDS, prices quoted by the bidder shall be fixed during the bidder's performance of the contract and shall not be subject to increases on any account. Submitted bids that are subject to price adjustment will be rejected. 15.2 The bidder may quote its prices for all Information Technologies, associated Goods, and Services to be supplied from outside Pakistan entirely in the currency or currencies approved by NBP. If the bidder wishes to be paid in a combination of different currencies, it must quote unit prices accordingly, but no more than two foreign currencies may be used. 15.3 Unless specified otherwise in the BDS, the bidder shall express its prices for such information technologies, associated goods, and services to be supplied locally (i.e., from within Pakistan).
16	Documents Establishing the Conformity of the Solution to	16.1 Pursuant to ITB clause 13.1 (f), the bidder shall furnish, as part of its bid, documents establishing the conformity to the Bidding Documents of the particular project that the bidder proposes to bid for. 16.2 The documentary evidence of conformity of the concerned project to the Bidding

	the Bidding Documents	Documents shall be in the form of written descriptions, literature, diagrams, certifications, and client references, including: a) the bidder's technical proposal, 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 with regard to the essential technical and performance characteristics of each component making up the proposed solution; b) The bidder shall submit an item-by-item commentary on the bidder's compliance with NBP's Technical Requirements in accordance with the format of Section-VI: Technical Requirement Sheet, demonstrating substantial responsiveness of the proposal 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, supporting documents, or other preprinted materials submitted with the bid, the item-by-item commentary shall prevail; c) A 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 other resources the bidder proposes to use. The project plan should include a detailed contract implementation schedule in bar chart form, showing the estimated duration, sequence, and interrelationship of key activities needed to complete the Contract Agreement. 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 from NBP, and any other party involved in the implementation of the project to provide during implementation and how the bidder proposes to coordinate the activities of all the parties involved; d) A written confirmation that the bidder accepts responsibility for the successful integration and interoperability of all components of the project as required by the Bidding Documents. 16.3 For the purposes of the commentary to be furnished pursuant to ITB clause 16.2 (b), the bidder shall note that references to brand names or model numbers, or national or proprietary standards designated by NBP in its Technical Requirements are intended to be descriptive and not restrictive. Except where explicitly prohibited in the BDS for specific items or standards, the bidder may substitute alternative brand/model names or standards in its bid, provided that it demonstrates to NBP's satisfaction that the use of the substitute(s) will result in the performance substantially equivalent to or better than that specified in the Technical Requirements.
17	Bid Security	17.1 Unless otherwise specified in the BDS, the bidder shall furnish, as part of its bid, a scanned bid security in the amount stipulated in the BDS. The hard copy of bid security must be submitted to NBP any time before the closing of bid submission. It is mandatory to enclose the bid security electronically in EPADS and submission of original hard copy physically to NBP before the closing of bid submission. Bids not following the aforementioned format will be rejected. 17.2 The bid security shall;

		a) at the bidder’s option, be in the form of either a certified cheque, letter of credit, or a bank guarantee from a banking institution; b) be issued by a reputable institution in Pakistan selected by the bidder; c) be substantially in accordance with one of the forms of bid security included in Section VII: Sample Forms or other form approved by NBP prior to bid submission; d) be payable promptly upon written demand by NBP in case any of the conditions listed in ITB clause 17.7 are invoked; e) be submitted in its original form, as copies shall not be accepted; f) remain valid for a period of at least 90-days and maximum 270-days beyond any extended period of bid validity subsequently requested pursuant to ITB clause 18.2. 17.3 The bid security of a joint venture shall be issued in the name of the joint venture submitting the bid and shall list all partners of the joint venture. 17.4 Any bid not accompanied by a substantially acceptable bid security in accordance with ITB clauses 17.2 and 17.3, shall be rejected by NBP as non-responsive. 17.5 The bid security may be forfeited: a) if a bidder: (i) withdraws its bid during the period of bid validity specified by the bidder on the Bid Form, except as provided in ITB clause 23.3 b) in the case of a successful bidder, if the bidder fails to: (i) sign the Contract Agreement in accordance with ITB clause 35; or (ii) Furnish performance security in accordance with ITB clause 36.
18	Period of Validity of Bids	18.1 Bids shall remain valid, at a minimum, for the period specified in the BDS after the deadline date for bid submission prescribed by NBP. A bid valid for a shorter period shall be rejected by NBP as non-responsive. Bidders are responsible for adjusting the dates in the BDS in accordance with any extensions to the deadline date of bid submission pursuant to ITB clause 21.2. 18.2 In exceptional circumstances, prior to expiry of the bid validity period, NBP may request the bidders to extend the period of validity for a specified additional period. The request and the responses to the request shall be made in writing. A bidder may refuse the request without forfeiting its bid security. A bidder agreeing to the request will not be permitted to modify its bid but will be required to extend the validity of its bid security correspondingly, pursuant to ITB clause 17.2 (f).

19	Format and Signing of Bid	19.1 The bidder shall prepare sets of documents in PDF file for the technical and financial bids specified in the BDS, clearly marking each one as "TECHNICAL PROPOSAL" "FINIANICAL PRPOSAL," etc., as appropriate. The bidder shall also enclose a bid security in the manner prescribed in ITB clause 17. 19.2 The documents in PDF file of the bid, each consisting of the documents listed in ITB clause 13.1, shall be typed, or written in readable fonts and shall be signed by a person or persons duly authorized to sign on behalf of the bidder. The authorization must be in writing and must be included in the bid pursuant to ITB Clause 13.1 (e). 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 person signing the bid. 19.3 The bid shall contain no interlineations, erasures, or overwriting, except to correct errors made by the bidder, in which case such corrections shall be initiated by the person or persons signing the bid. 19.4 The bidder shall furnish in the Bid Form (a sample of which is provided in the Sample Forms Section of the Bidding Documents) information regarding commissions or gratuities, if any, paid or to be paid to agents in relation to this procurement and the execution of the Contract Agreement, should the bidder be successful.

D. Submission of Bids

20	Electronic Bidding	20.1 The bidder shall submit electronic bids as per the requirements of e-procurement systems EPADS. 20.2 In case of Single Stage Two Envelopes Procedure, the bid shall comprise two bids submitted electronically simultaneously, one called the "Technical Proposal" and the other "Financial Proposal."
21	Deadline for submission of Bids	21.1 Bids must be submitted electronically through EPADS as specified in the BDS for ITB not later than the date and time intimated by NBP. 21.2 NBP may extend this deadline for submission of bids by amending the bidding documents in accordance with ITB clause 11.3, in which case all rights and obligations of NBP and the bidders will thereafter be subject to the deadline as extended.
22	Late Bids	22.1 Any bid received by NBP after the bid submission deadline prescribed by NBP in the BDS for ITB clause 21, will be rejected and returned unopened to the bidder.
23	Modification or Withdrawal of Bids	23.1 The bidder may modify or withdraw its bid after submission, through EPADS prior to the deadline prescribed for bid submission. 23.2 Revision of bid may be submitted electronically through EPADS after withdrawal of original bid before the deadline of submission of bid. 23.3 No bid may be modified after the deadline of submission of bids. 23.4 No bid may be withdrawn in the interval between the bid submission deadline and the expiration of the bid validity period specified in ITB clause 18. Withdrawal of a bid during this interval may result in the forfeiture of the bidder's bid security, pursuant to ITB clause 17.7.

Bid Opening and Evaluation

24	Opening of Bids by NBP	24.1 NBP shall open electronically through EPADS all technical proposals for all packages, excluding withdrawals, in public, in the presence of bidders' representatives who choose to attend, at the time, on the date and at the place specified in the BDS. Bidders' representatives shall sign a register as proof of their attendance. 24.2 The procuring agency should open and evaluate the technical proposal first, without opening the financial proposal and without reference to the price and reject any proposal which does not conform to the specified technical requirements. 24.3 The financial proposals shall retain unopened in EPADS; 24.4 During the technical evaluation no amendments to the technical proposal shall be permitted. 24.5 After the evaluation and approval of the technical proposal the procuring agency, shall at a time within the bid validity period, publicly open the financial proposals electronically through EPADS of the technically accepted bids only. The financial proposal of bids found technically non-responsive shall not be opened. 24.6 Financial proposals shall be opened one at a time. The following details shall be read out: a) Unit Price; and b) Bid Amount 24.4 NBP shall prepare minutes of the bid opening, including the information disclosed to those present in accordance with ITB clause 24.3.
25	Clarification of Bids	25.1 During the bid evaluation, NBP may, at its discretion, ask a bidder for a clarification of its bid. The request for clarification and the response shall be in writing, and no change in the price or substance of the bid shall be sought, offered, or permitted.
26	Preliminary Examination	26.1 NBP shall examine the technical proposals to determine whether: i) They are complete in all respects. ii) the documents have been properly signed; and iii) whether the bids are generally in order. 26.2 In case of a pre-qualification process having been undertaken for the contract(s) for which these Bidding Documents have been issued, NBP shall ensure that each bid is from a pre-qualified bidder, and in the case of a joint venture, the partners and structure of the joint venture are unchanged from those in the pre-qualification. Bidder's profile, technical compliance, major and minor deviations from the given specifications, solution offered as and where applicable will be individually listed and duly evaluated. 26.3 NBP may waive any minor formality, nonconformity, or irregularity in a bid that does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder. 26.4 Prior to the detailed evaluation, NBP shall determine whether each bid is of acceptable quality, complete, and substantially responsive to the Bidding Documents. For purposes of this determination, a substantially responsive bid is one that conforms to all the terms, conditions, and specifications of the Bidding Documents without material deviations, exceptions, objections, conditional ties, or reservations. A material deviation, exception, objection, conditionality, or reservation is one: (i) that limits in any substantial way, the scope, quality, or performance of the project; or (ii)

		is inconsistent with the Bidding Documents or limits in a substantial way, NBP's rights or the successful bidder's obligations under the Contract Agreement; or (iii) the acceptance of which would unfairly affect the competitive position of other bidders who have submitted substantially responsive bids. 26.5 If a bid is not substantially responsive, it shall be rejected by NBP and may not subsequently be made responsive by the bidder by correction of the nonconformity. NBP's determination of bid responsiveness shall be based on the contents of the bid itself.
27	Conversion to Single Currency	27.1 For evaluation and comparison purposes, NBP shall convert all bid prices expressed in various currencies and amounts into a single currency specified in the BDS, using the selling rate prevailing on the date of opening of the bids intimated by NBP, as notified by the State Bank of Pakistan.
28	Evaluation Criteria	28.1 Bids for sub-systems, or slices of the overall Information System will be accepted if specified in the BDS. 28.2 The bid evaluation shall be carried out in accordance with fulfillment of the specifications/requirements specified in Section-VI and the bid evaluation criteria specified in Section-VII "Technical Evaluation Criteria".
29	Domestic Preference	29.1 If indicated in the BDS and as per PPRA Rule 24, NBP shall grant a margin of preference for use of domestic Information Technologies and related Goods. Under this preference, for Goods supplied from outside Pakistan, the CIP (named place of destination) price shall be increased by the applicable import tariff (custom duties and other import taxes) or fifteen (15) percent, whichever is less. If duties vary from item to item within the bid, the appropriate tariff for each item shall apply. No preference shall be applied for any associated Services or works components of the bid. 29.2 No margin of preference will be granted for any other price component, and bidders will not be permitted or required to modify the source of any hardware, Software, related equipment, materials, products, or other Goods, as well as related Services after bid opening.
30	Contacting NBP	30.1 From the time of bid opening to the time of the announcement of the successful bidder, if any bidder wishes to contact NBP on any matter related to the bid, it should do so in writing. 30.2 If a bidder tries to directly influence NBP or otherwise interfere in the bid evaluation process and the decision to select a bidder as the successful bidder, its bid may be rejected.

E. Post Evaluation Criteria and Award of Contract

31	Post Evaluation Criteria	31.1 NBP will determine at its own cost and to its satisfaction whether the bidder which is selected as having submitted the most advantageous bid is qualified to perform the Contract Agreement satisfactorily, in accordance with ITB clause 6. If a pre-qualification process was undertaken for the Contract Agreement and/ or related agreements for which these Bidding Documents were issued, NBP will determine in the manner described above that no material changes have occurred after the pre-qualification that negatively affects the ability of the bidder which has submitted the most advantageous bid to perform the Contract. 31.2 Pursuant to ITB clauses 6 and 16, the evaluation of the bidder's financial, technical, design, integration, customization, production, management, and support capabilities will be based on an examination of the documentary evidence of the bidder's qualifications, as well as other information which NBP deems necessary and appropriate. This evaluation may include visits or interviews with the bidder's clients referenced in its bid, site inspections, and any other measures. NBP may, at its discretion, also carry out tests to determine whether the performance or functionality of the solution offered meets those stated in the technical requirements before announcement of the successful bidder. 31.3 An affirmative post-qualification evaluation will be a prerequisite for selecting the most advantageous bidder. A negative evaluation will result in rejection of the bidder's bid, in which event NBP shall proceed to the next most advantageous bidder to make a similar evaluation of that bidder's capabilities to perform satisfactorily.
32	Award Criteria	32.1 Subject to ITB clause 33, NBP shall award the contract to the bidder whose bid has been evaluated and determined to be substantially responsive and the most advantageous bid, provided further that the bidder has been determined to be qualified to perform the contract satisfactorily, pursuant to ITB clause 31.
33	NBP's Right to Accept any Bid and to Reject any or all Bids	33.1 NBP reserves the right to annul the bidding process as per PPRA Rule 33 and reject all bids at any time prior to the execution of the Contract Agreement with the successful bidder, without thereby incurring any liability to the bidders.
34	Notification of Award	34.1 Prior to the expiration of the period of bid validity, NBP shall notify the successful bidder in writing by registered letter, or by electronic means, including the PPRA and NBP websites, to be subsequently confirmed in writing by registered letter, that its bid has been accepted. 34.2 The contract with the successful bidder shall come into force as follows: a) where no formal signing of a contract is required, from the date the notice of the acceptance of the bid or purchase order has been given to the bidder whose bid has been accepted. Such notice of acceptance or purchase order shall be issued within a reasonable time; or; b) where the procuring agency requires signing of a written contract, from the date on which the signatures of both the procuring agency and the successful bidder we affixed to the written contract. Such affixing of signatures shall take place within a reasonable time. 34.3 Provided that when the coming into force of a contract is contingent upon fulfilment of a certain condition or conditions, the contract shall take effect from

		the date whereon such fulfilment takes place. 34.4 When the successful bidder furnishes the signed Contract Agreement between the bidder and NBP and the performance security pursuant to ITB clause 37, NBP shall notify each unsuccessful bidder and will discharge their bid security.
35	Signing of Contract	35.1 At the same time as NBP notifies the successful bidder that its bid has been accepted, NBP shall negotiate as per PPRA Rule 40 and finalize a contract based on the form of contract attached hereto with the bidder which shall set out the understanding and agreement between the parties relating to the transaction/project. If required by the demands of the project and its legal implications, the bidder and NBP may enter into several contracts on different aspects of the transaction/project. 35.2 Following notification of the award of the contract, NBP and the successful bidder shall sign and date the formal Contract Agreement as soon as practically possible. Provided, however, that NBP may in its discretion extend the date for signing the formal contract.
36	Performance Security	36.1 The successful bidder shall furnish the performance security in accordance with the GCC, using the performance security bank guarantee form provided in the Bidding Documents or another form acceptable to NBP at the time of signing of the Contract Agreement. 36.2 Failure of the successful bidder to comply with the requirements of ITB clause 35 or ITB clause 36.1 shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event NBP may make the award to the next most advantageous bid submitted by a qualified bidder or call for new bids.

3. BID Data Sheet – BDs (Section-III)

The following specific information relating to LOS - Request for Proposal that will be used shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions in the Bid Data Sheet (BDS) shall prevail over those mentioned in the ITB.

A. General

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 The Description (as specified in Section VII) of the System is: LOS - Request for Proposal Please refer to the delivery schedule in Section XI – Delivery Schedule The commencement date for delivery: Please refer to the delivery schedule in Section XI – Delivery Schedule
2.	2.1 & 2.2	Financial year for the operations of the Procuring Agency: 2025 Name of Project: LOS - Request for Proposal for 3 Years (extendable) as per the requirements mentioned in Section-VII Technical Requirements attached separately with the bidding documents. • Name of financing institution: National Bank of Pakistan • Name and identification number of the Contract As mentioned on the NBP & PPRA website
3.	3.1	A Joint Venture is applicable. In Case Yes, the Maximum number of members in the joint venture shall be [2].
4.	4.6	Demonstration of authorization by manufacturer: Re*quired*
Note: For this tender, NBP has used the Standard Bidding Documents provided for the Information System by the Public Procurement Regulatory Authority. However, all references 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 - muhammad.asad@nbp.com.pk		
5.	8.1	All the clarifications and their responses shall be made through EPADS.

B. Preparation of Bids

1.	7.2	The required documents shall be uploaded on EPADS
2.	8.1	All the clarifications and their responses shall be made through EPADS.
	8.5	Pre-bid meeting: Not Required

C. Preparation of Bids

1.	10.1	The Language of all correspondences and documents related to the Bid is: English
2.	11.1 (h)	In addition to the documents stated in ITB 11, the following documents must be included with the Bid All technical product documents mentioned in Section V
3.	12.3 (c)	Other procurement-specific documentation requirements are: [As per the technical requirement document for evidence of mandatory technical requirements].
4.	12.4	Spare parts: Not Applicable
5.	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 Information System, that it has been duly authorized to deliver, in Pakistan, the Information System indicated in its Bid.
6.	15.6 (a) (iii), (iv) (optional)	For goods making information Systems manufactured from within Pakistan the price quoted shall ONLY be in PKR (Pakistani Rupee)
7.	15.6 (a) (i) & 15.6 (b) (i)	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.
8.	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)
9.	16.1 (a)	a) For Information 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.
10.	16.2	For the purpose 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.
11.	17.1	The Bid Validity period shall be *270* days.
12.	18.1	The amount of Bid Security shall be Rs. 1,232,000/-

		The currency of the Bid Security shall be in Pakistani Rupees [PKR]
13.	18.3	The Bid Security shall be furnished as a certified cheque, pay order, or bank guarantee, issued by a recognized banking institution. The prescribed format for the bank guarantee is provided in Section XII, Standard Forms.
14.	18.3 (c)	Other forms of security are: NA
15.	19.1	Alternative Bids to the requirements of the Bidding Documents will not be permitted.
16.	21.1	The number of copies of the Bid to be completed and returned shall be *01.*
17.	21.2	Written confirmation of authorization are: Letter of authorization to sign the contract & Submit a proposal on behalf of the bidding company signed by the CEO or board resolution.

D. Submission of Bids

1.	22.2 (a)	The bid shall be uploaded on EPADS. (Scan Copy) The address for submission of the original Bid Security is: The Divisional Head – Procurement Division, LCMG, 3rd Floor, National Bank of Pakistan, Head Office, I.I. Chundrigar Road, Karachi. Street address: *NBP – Head Office* Building/Plot No. *[insert Building/Plot]* Floor/Room No.:*3rd* City/Town: *Karachi*
2.	22.2 (b)	Title of the subject Procurement or Project name: *Loan Origination System* ITB No: *Please refer to websites (NBP & PPRA)* Time and date for submission*:* June 17th, 2025, *03:00 PM*
3.	23.1	The deadline for Bid submission is a) Day*: Tuesday* b) Date*:* June 17th, 2025 c) Time*:* 03:00 PM

E. Opening and Evaluation of Bids

1.	26.1	The Bid opening shall take place at EPADS.
2.	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 the 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 The exchange rate of the date of opening will be used for evaluation.
3.	33.4 (h)	Other specific criteria are [as per the detailed Technical and Payment section]
4.	33.5 (a)	Inland transportation from EXW/port of entry/border point to *[name of Project site(s)]*, and insurance and incidentals. Please refer to the bidder qualification criteria in section VIII.
5.	33.5 (b)	Delivery schedule. Within 24 weeks after the signing of the contract or as per the mutual agreement between the bidder and NBP
6.	33.5 (c) (ii)	Deviation in payment is *not applicable*
7.	33.5 (d)	Cost of spare parts. *Please refer to section X BOQ*
8.	33.5(e)	Spare parts and after-sales service facilities in Pakistan. (*Please refer to section X BOQ*)
9.	33.5 (f)	Operating and maintenance costs. Factors for calculation of the whole life cost: *Please refer to section X BOQ*
10.	33.5 (g)	Performance and productivity of Information System. *Please refer to section X BOQ.*
11.	33.5 (h)	Specific additional criteria to be used in the evaluation and their evaluation method: Please refer to section X BOQ, Technical Specification and Bidder criteria, Delivery Schedule and Payments terms
12.	33.6	In case of an 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 VIII.

13.	34.1	a) Domestic preference to apply. Preference to domestic or national suppliers or contractors shall be provided in accordance with the policies of the Federal Government and/or in accordance with the regulations issued by the Authority.
14.	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 VIII – Evaluation Criteria, Qualification Criteria and Technical Evaluation

F. Award of Contract

1.	40.1	The percentage for quantity increase or decrease is Not applicable, however, please refer to section X
2.	43.1	The Performance Security (Guarantee) shall be 05% of the total quoted amount of the qualified bidder.
3.	43.2	The Performance Guarantee shall be in the form of a Bank Guarantee.
4.	44.2	The maximum amount of Advance payment shall be 05% against advance bank guarantee, please refer to section IX payment plan.
5.	45.1	An arbitrator shall be appointed by mutual consent of both parties.

G. Review of Procurement Decisions

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

4. Eligible Countries (Section-IV)

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

The following countries are ineligible to participate in the procurement process:

1. India
2. Israel

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

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

5. General Conditions of Contract (Section-V)

The General Conditions of Contract ("GCC") contained in this section are to be read in conjunction with the Special Conditions of Contract ("SCC") and conditions of the Contract Agreement (as defined herein below) which will be executed between NBP and the Supplier. The aforesaid GCC, SCC and the Contract Agreement shall form a complete document expressing all the rights and obligations of the parties; however, the Contract will be finalized in consultation with the Supplier and Legal Department of NBP. The GCC must remain unaltered. Contract -specific information, deletions, extensions, and modifications to the GCC shall be introduced through the SCC and the Contract Agreement. In the event of any conflict between the terms of the GCC, the SCC and the Contract Agreement, the terms of the Contract Agreement shall prevail.

A. Contract and Interpretation

1	Definitions	1.1 The following terms shall be interpreted as indicated below. a) Contract elements: (i) "Contract Documents" means the documents specified in Article 1.1 (Contract Documents) of the form of a contract agreement (including any amendments to these Documents). (ii) "Contract Agreement" means the agreement entered between NBP and the Supplier using the form of contract agreement contained in the sample forms section of the bidding documents and any modifications to this form agreed to by NBP and the Supplier, including any novation's, modifications, or amendments thereto. (iii) "GCC" means the General Conditions of Contract. (iv) "SCC" means the Special Conditions of Contract. (v) "Technical Requirements" means the Technical Requirements section of the bidding documents. (vi) "Implementation Schedule" means the Implementation Schedule sub-section of the Technical Requirements. (vii) "Contract Price" means the price or prices stated in the Contract Agreement. (viii) "Bidding Documents" refers to the collection of documents issued by NBP to instruct and inform potential Suppliers of the processes for bidding, selection of the most advantageous bid, and contract formation, as well as the contractual conditions governing the relationship between NBP and the Supplier. The GCC, the SCC, the Technical Requirements, and all other documents included in the Bidding Documents reflect the procurement guidelines that NBP is obligated to follow during procurement and administration of the process for the formalization of the Contract Agreement and its performance. b) Entities: (i) "NBP" means NBP. (ii) "Project Manager" means the person appointed by NBP in the manner provided in GCC Clause 18.1 (Project Manager) and named as such in

the SCC to perform the duties delegated by NBP.

(iii) "Supplier" means the person(s) whose bid to perform the contract has been accepted by NBP and is named as such in the Contract Agreement.

(iv) "Supplier's Representative" means any person nominated by the Supplier and named as such in the Contract Agreement and approved by NBP in the manner provided in GCC Clause 18.2 (Supplier's Representative) to perform the duties delegated by the Supplier in connection with the performance of the Contract Agreement.

(v) "Subcontractor," including Bidder, means any person to whom any of the obligations of the Supplier, including preparation of any design or supply of any Information Technologies or other Goods, software, or Services, is subcontracted directly or indirectly by the Supplier.

c) Scope

(i) "Solution" also called the "System/software" means all the Information Technologies, Materials, and other Goods to be supplied, installed, integrated, and made operational, together with the LOS - Request for Proposal provision as per international standards to be carried out by the Supplier under the Contract. For the avoidance of any doubt the term "System" includes any Sub-system.

(ii) "Sub-system" means any sub-set of the System identified as such in the Contract Agreement that may be supplied, installed, tested, and commissioned individually before commissioning the entire System.

(iii) "Information Technologies" means all information processing and communications-related hardware, Software, supplies, and consumable items that the Supplier is required to supply and install under the Contract Agreement.

(iv) "Goods" means all equipment, machinery, furnishings, Plastic, stationary, Materials, and other tangible items that the Supplier is required to supply or supply and install under the Contract Agreement, including, without limitation, the Information Technologies, and Materials.

(v) "Services" means all technical, logistical, management, and any other Services to be provided by the Supplier under the Contract Agreement to supply, install, customize, integrate, and make the System operational. Such Services may include but are not restricted to, activity management and quality assurance, design, development, customization, documentation, transportation, insurance, inspection, expediting, site preparation, installation, integration, training, data migration, pre-commissioning, commissioning, maintenance, and technical support.

(vi) "Project Plan" means the document to be developed by the Supplier and approved by NBP, according to GCC clause 19, based on the requirements of the Contract Agreement and the Preliminary Project Plan included in the Supplier's bid. The "Finalized Project Plan" is the version of the Project Plan approved by NBP, following GCC clause 19.2. Should the Project Plan conflict with the Contract Agreement in any way, the relevant provisions of the Contract Agreement, including any amendments, shall prevail.

(vii) "Software" means that part of the System which are instructions that cause the information processing Sub-systems to perform in a specific manner or execute specific operations.

(viii) "System Software" means Software that provides the operating and management instructions for the underlying hardware and other components and is identified as such in the Contract Agreement and such other Software as the parties may agree in writing to be Systems Software. Such System Software includes but is not restricted to, micro-code embedded in hardware (i.e., "firmware"), operating systems, communications, system and network management, and utility software.

(ix) "General-purpose software" means Software that supports general-purpose office and software development activities and is identified as such in the Contract Agreement and such other Software as the parties may agree in writing to be General-Purpose Software. General-purpose software may include but is not restricted to word processing, spreadsheets, generic database management, and application development software.

(x) "Application Software" means Software formulated to perform specific business or technical functions and interface with the business or technical users of the System and is identified as such in the Contract Agreement and such other Software as the parties may agree in writing to be Application Software.

(xi) "Standard Software" means Software identified as such in the Contract Agreement and such other Software as the parties may agree in writing to be Standard Software.

(xii) "Custom Software" means Software identified as such in the Contract Agreement and such other Software as the parties may agree in writing to be Custom Software.

(xiii) "Source Code" means the database structures, dictionaries, definitions, program source files, and any other symbolic representations necessary for the compilation, execution, and subsequent maintenance of the Software (typically, but not exclusively, required for Custom Software).

(xiv) "Materials" means all documentation in printed or printable form and all instructional and informational aides in any form (including audio, video, and text) and on any medium, provided to NBP under the Contract Agreement.

(xv) "Standard Materials" means all Materials not specified as Custom Materials.

(xvi) "Custom Materials" means Materials developed by the Supplier i.e., Cards Plastic, Stationary, etc. under the Contract Agreement and identified as such in the Contract Agreement or any related agreement between the parties (if any) and such other Materials as the parties may agree in writing to be Custom Materials. Custom Materials include Materials created from Standard Materials.

(xvii) "Intellectual Property Rights" means any copyright, trademark, patent, and other intellectual and proprietary rights, title, and interests worldwide, whether vested, contingent, or future, including without limitation, all economic rights and all exclusive rights to reproduce, fix, adapt, modify, translate, create derivative works, extract or re-utilize data, manufacture, introduce into circulation, publish, distribute, sell, license, sublicense, transfer, rent, lease, transmit or provide electronic access, broadcast, display, enter into computer memory, or otherwise use any portion or copy, in whole or in part, in any form, directly or indirectly, or to authorize or assign others to do so.

(xviii) "Supplier's Equipment" means all equipment, tools, apparatus, or things of every kind required in or for installation, completion, and maintenance of the System that is to be provided by the Supplier, excluding the Information Technologies, or other items forming part of the System.

d) Activities

(i) "Delivery" means the transfer of the Goods from the Supplier to NBP following the current edition Incoterms specified in the Contract Agreement. "Incoterms" means international commercial terms published by the International Chamber of Commerce (ICC).

(ii) "Installation" means that the System or a Subsystem, as specified in the Contract, is ready for Commissioning as provided in GCC clause 26 (Installation).

(iii) "Pre-commissioning" means the testing, checking, and any other required activity that may be specified in the Technical Requirements that are to be carried out by the Supplier in preparation for the Commissioning of the System as provided in GCC clause 26 (Installation).

(iv) "Commissioning" means the operation of the System or any Subsystem by the Supplier following Installation, which is to be carried out by the Supplier as provided in GCC clause 27.1 (Commissioning), to carry out Operational Acceptance Test(s).

(v) "Operational Acceptance Tests" means the tests specified in the Technical Requirements and the Finalized Project Plan to be carried out to ascertain whether the System or a specified Subsystem, can attain the functional and performance requirements specified in the Technical Requirements and the Finalized Project Plan, following the provisions of GCC clause 27.2 (Operational Acceptance Test).

(vi) "Operational Acceptance" means the acceptance by NBP of the System (or any Subsystem(s) where the Contract Agreement provides for acceptance of the System in parts), following GCC clause 27.3 (Operational Acceptance).

e) Place and Time

(i) "Pakistan" is the country named in the SCC.

(ii) "Supplier's Country" is the country in which the Supplier is legally organized, as named in the Contract Agreement.

(iii) "Project Site(s)" means the place(s) specified in the SCC and /or the Contract Agreement for the Cards Stationary & supply and installation of the System (if required in the agreement).

(iv) " Eligible Country" shall mean any country except Israel, a country subject to sanctions of the United Nations, and any country subject to trade and

		commercial restrictions by the Federal Government of Pakistan. (v) "Day" means a calendar day in the Gregorian Calendar. (vi) "Week" means seven (7) consecutive days, beginning on the first Day of the week as is customary in Pakistan. (vii) "Month" means a calendar month in the Gregorian Calendar. (viii) "Year" means twelve (12) consecutive months. (x) "Contract Period" is the tenor of the Contract Agreement. (xi) "Defect Liability Period" (also referred to as the "Warranty Period") means the period of validity of the warranties given by the Supplier commencing on the date of the Operational Acceptance certificate of the System or Subsystem(s), during which the Supplier is responsible for defects concerning the System (or the relevant Sub-system(s)) as provided in GCC clause 29 (Defect Liability). (xii) "Post-Warranty Services Period" means the number of years defined in the SCC (if any), following the expiration of the Warranty Period during which the Supplier may be obligated to provide Software licenses, maintenance, and/or technical support services for the System, either under the Contract Agreement or under a separate contract(s). (xiii) "The Coverage Period" means the Days of the Week and the hours of those Days during which maintenance, operational, and/or technical support services (if any) must be available.
2	Contract Documents	2.1 All documents forming part of the Contract Agreement (and all parts of these documents) are intended to be correlative, complementary, and mutually explanatory. The Contract Agreement shall be read as a whole along with the GCC and the SCC.
3	Interpretation	3.1 Language: a) All Contract Documents, all correspondence, and communications to be given shall be written in the language specified in the SCC, and the Contract Agreement shall be construed and interpreted following that language. b) If any of the Contract Documents, correspondence, or communications are prepared in any language other than the governing language under GCC clause 3.1.1 above, the translation of such documents, correspondence, or communications shall prevail in matters of interpretation. The originating party shall bear the costs and risks of such translation, concerning such documents, correspondence, and communications. 3.2 Singular and Plural: The singular shall include the plural, and the plural shall include the singular, except where the context requires otherwise. 3.3 Headings: The headings and marginal notes in the GCC are included for ease of reference and shall neither constitute a part of the Contract nor affect its interpretation. 3.4 Persons: Words importing persons or parties shall include individuals, firms, companies, corporations, and government entities. 3.5 Entire Agreement: The Contract Agreement shall constitute the entire agreement between NBP and the Supplier, when executed, concerning the subject matter of The Contract Agreement and shall supersede all communications, negotiations, and agreements (whether written or oral) of the parties concerning the subject

		matter of the Contract Agreement made before the date of Contract Agreement, unless such communications, negotiations, and agreements are expressly incorporated into the Contract Agreement. 3.6 Amendment: No amendment or other variation of the Contract Agreement shall be effective unless it is in writing, is dated, expressly refers to the Contract Agreement, and is signed by a duly authorized representative of each party to the Contract Agreement. 3.7 Independent Supplier: The Supplier shall be an independent contractor carrying out the Contract Agreement. The Contract Agreement does not create any agency, partnership, joint venture, or other joint relationship between the parties to the Contract Agreement. Subject to the provisions of the Contract Agreement, the Supplier shall be solely responsible for how the Contract Agreement is performed. All employees, representatives, or Subcontractors engaged by the Supplier in connection with the performance of the Contract Agreement shall be under the complete control of the Supplier and shall not be deemed to be employees of NBP and nothing contained in the Contract Agreement, or any subcontract awarded by the Supplier shall be construed to create any contractual relationship between any such employees, representatives, or Subcontractors and NBP. 3.8 Joint Venture or Consortium: If the Supplier is a joint venture or consortium of two or more persons, all such firms shall jointly and severally be bound to NBP for the fulfillment of the provisions of the Contract Agreement and shall designate one of such persons to act as a leader with authority to bind the joint venture or consortium. The composition or constitution of the joint venture or consortium shall not be altered without the prior consent of NBP. 3.9 Non-waiver: a) Subject to GCC clause 3.9.2 below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract Agreement or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract Agreement, nor shall any waiver by either party of any breach of Contract Agreement operate as a waiver of any subsequent or continuing breach of Contract Agreement. b) Any waiver of a party's rights, powers, or remedies under the Contract Agreement must be in writing, must be dated and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived. 3.10 Severability: If any provision or condition of the Contract Agreement is prohibited or rendered invalid or unenforceable, such prohibition, invalidity, or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract Agreement.
4	Notices	4.1 Unless otherwise stated in the Contract Agreement, all notices to be given under the Contract shall be in writing and shall be sent by personal delivery, courier, facsimile, electronic mail, or Electronic Data Interchange (EDI) to the address of the relevant party as specified in the SCC, with the following provisions. 4.1.1 Any notice sent by facsimile, electronic mail, or EDI shall be confirmed within two (2) days after dispatch by notice sent by courier, except as otherwise specified in the Contract Agreement.

		4.1.2 Any notice sent by courier shall be deemed (in the absence of evidence of earlier receipt) to have been delivered ten (10) Days after dispatch. In proving the fact of dispatch, it shall be sufficient to show that the envelope containing such notice was properly addressed, stamped, and conveyed to the courier service for transmission by courier. 4.1.3 Any notice delivered personally or sent by facsimile, electronic mail, or EDI shall be deemed to have been delivered on the date of its dispatch. 4.1.4 Either party may change its postal, facsimile, electronic mail, or EDI address or addressee for receipt of such notices by ten (10) Days' notice to the other party in writing. 4.2 Notices shall be deemed to include any approvals, consents, instructions, orders, and certificates to be given under the Contract Agreement.
5	Governing Law	5.1 The Contract Agreement shall be governed by and interpreted following the laws of the country specified in the SCC.
6	Settlement of Disputes	6.1 Negotiations: a) If a dispute of any kind whatsoever shall arise between NBP and the Supplier in connection with or arising out of the Contract Agreement, including without prejudice to the generality of the foregoing, any question regarding its existence, validity, or termination, or the execution of the project (whether during the progress of implementation or after its achieving Operational Acceptance, and whether before or after the termination, abandonment, or breach of the Contract Agreement), the parties shall seek to resolve any such dispute or difference by mutual consultation. b) If the parties fail to resolve such a dispute or difference by mutual consultation, within fourteen (14) Days after one party has notified the other in writing of the dispute or difference, then, each of the parties may refer the matter for arbitration. 6.2 Arbitration: a) A party shall give notice to the other party of its intention to commence arbitration, as provided below, as to the matter in dispute, and no arbitration in respect of this matter may commence unless such notice is given. b) Any dispute in respect of which a notice of intention to commence arbitration has been given, following GCC clause 6.2.1 shall be finally settled by arbitration. Arbitration may commence before, during, or after the completion of the project. c) Arbitration proceedings shall be conducted following the rules of procedure specified in the SCC. d) Notwithstanding any reference to arbitration in this clause the parties shall continue to perform their respective obligations under the Contract Agreement unless they otherwise agree.

B. Subject Matter of Contract

7	Scope of the System	7.1 Unless otherwise expressly limited in the SCC or Technical Requirements, the Supplier's obligations cover the provision of **LOS - Request for Proposal**, inventory, stationary, Materials, and other related material as per standards and any other

		documents specified in the Contract Agreement and the Finalized Project Plan. 7.2 The Supplier shall, unless specifically excluded in the Contract Agreement, perform all such work and/or supply all such items and Materials not specifically mentioned in the Contract Agreement but that can be reasonably inferred from the Contract Agreement 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 Agreement. 7.3 The Supplier's obligations (if any) to provide Plastic, stationary, inventory, Goods and Services, etc. as per international standards (e.g., issuance, personalization, technical assistance, and operational support), are specified in the SCC, including the relevant terms, characteristics, and timings.
8	Timelines	8.1 The Supplier shall commence work on the solution within the period specified in the SCC, and without prejudice to GCC clause 28.2, the Supplier shall thereafter proceed with the solution following the schedule specified in the Implementation Schedule in the Technical Requirements section and any refinements made in the Finalized Project Plan. 8.2 The Supplier shall achieve Operational Acceptance of the LOS - Request for Proposal within the time specified in the SCC following the schedule specified in the Implementation Schedule in the Technical Requirements Section and any refinements made in the Finalized Project Plan, or within such extended time to which the Supplier shall be entitled under GCC clause 40 (Extension of Time for Achieving Operational Acceptance).
9	Supplier Responsibilities	9.1 The Supplier shall conduct all activities with due care and diligence following the Contract Agreement and with the skill and care expected of a competent provider of solutions and related services following 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. 9.2 The Supplier confirms that it has entered into this Contract Agreement based on a proper examination of the information and specifications relating to the System provided by NBP and based on information that the Supplier could have obtained from a visual inspection of the Project Site (if access to the site was available) and other data readily available to the Supplier relating to the System. 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 Agreement. 9.3 The Supplier shall be responsible for the timely provision of all resources, information, and decision-making under its control that are necessary to reach a mutually agreed Finalized Project Plan (pursuant to GCC clause 19.2) within the 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 41.2. 9.4 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 Pakistan and other relevant jurisdictions including but not limited to the country where the Supplier is incorporated, 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 permits, approvals, and/or licenses that are necessary for the performance of the Contract Agreement. 9.5 The Supplier shall comply with all laws in force in Pakistan and other relevant jurisdictions including but not limited to the country where the Supplier is incorporated. The laws will include all national, provincial, municipal, or other laws that affect the performance of the Contract Agreement and are binding upon the Supplier. The Supplier shall indemnify and hold harmless NBP from and against any 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. The Supplier shall not indemnify NBP to the extent that such liability, damage, claims, fines, penalties, and expenses were caused by a fault of NBP. 9.6 The Supplier shall pay due regard to all recognized festivals, official holidays, religious or other customs, and all local laws and regulations about the employment of labor in all dealings with its labor and the labor of its Subcontractors currently employed in connection with the Contract Agreement. 9.7 Any Information Technologies or other Goods and Services that will be incorporated in or be required for the Solution and other supplies shall have their origin in an Eligible Country. 9.8 The Supplier shall permit the Bank to inspect the Supplier's accounts and records relating to the performance of the Supplier and to have them audited by auditors appointed by the Bank if so, required by the Bank. 9.9 Other Supplier responsibilities, if any, are as stated in the SCC.
10	NBP's Responsibilities	10.1 NBP shall ensure the accuracy of all information and/or data to be supplied by NBP to the Supplier, except when otherwise expressly stated in the Contract Agreement. 10.2 NBP shall be responsible for the timely provision of all resources, information, and decision-making under its control that are necessary to reach an agreed Finalized Project Plan (pursuant to GCC clause 19.2) within the schedule specified in the Implementation Schedule in the Technical Requirements section. 10.3 NBP 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 Agreement which is to be agreed by mutual consent. 10.4 NBP assumes primary responsibility for the Operational Acceptance Test(s) for the System following GCC clause 27.2. 10.5 NBP is responsible for performing and safely storing timely and regular backups of its data and Software following accepted data management principles, except where such responsibility is assigned to the Supplier as per in the Contract Agreement. 10.6 All costs and expenses involved in the performance of the obligations of NBP under this GCC clause 10 shall be the responsibility of NBP, save those to be incurred by the Supplier concerning the performance of the Operational Acceptance Test(s), following GCC clause 27.2. 10.7 Other NBP responsibilities, if any, are as stated in the SCC.

C. Payment

11	Contract Price	11.1 The Contract Price shall be as specified in the Contract Agreement. 11.2 The Contract Price shall be a firm lump sum not subject to any alteration, except: a) in the event of a Change in the System pursuant to GCC clause 39 or other clauses in the Contract Agreement; or b) Following the price adjustment formula (if any) specified in the SCC. 11.3 The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of the Contract Price, which shall, except as otherwise provided for in the Contract Agreement, cover all its obligations under the Contract Agreement.
12	Terms of Payment	12.1 The Supplier's request for payment shall be made to NBP in writing, accompanied by an invoice describing, as appropriate, the System or Sub-system(s), delivered, Pre-commissioned, Installed, and Operationally Accepted, and by documents submitted pursuant to GCC clause 22.5 and upon fulfillment of other obligations stipulated in the Contract Agreement. 12.2 No payment made by NBP herein shall be deemed to constitute acceptance by NBP of the System or any Subsystem(s). 12.3 Payments shall be made promptly by NBP, but in no case later than thirty (30) Days after submission of a valid invoice by the Supplier. In the event that NBP fails to make any payment by its respective due date or within the period outlined in the Contract Agreement, NBP shall pay to the Supplier interest on the amount of such delayed payment at the rate(s) specified in the SCC for the period of delay until payment has been made in full, whether before or after judgment or arbitration award. 12.4 All payments shall be made in the currency (ies) specified in the Contract Agreement, pursuant to GCC clause 11. For Goods and Services supplied locally, payments shall be made in the currency of Pakistan, unless otherwise specified in the SCC.
13	Securities	13.1 Advance Payment Security: a) As specified in the SCC, the Supplier shall provide security equal in amount and currency to the advance payment. Except as provided otherwise in the Contract Agreement, the security shall be valid until the System is Operationally Accepted. b) The security shall be in the form provided in the Bidding Documents or another form acceptable to NBP. The security shall be returned to the Supplier immediately after its expiration. 13.2 Performance Security: a) The Supplier shall, within **twenty-eight (28) Days** of the notification of the award of the contract to the successful bidder, provide security for the due performance of the Contract Agreement in the amount and currency specified in the SCC. b) The security shall be a bank guarantee, substantially in the form provided in the Sample Forms section of the Bidding Documents, or such other form as may be acceptable to NBP. c) The security shall become null and void once all the obligations of the Supplier under the Contract Agreement have been fulfilled to the satisfaction of NBP or

		following the criteria specified in the Contract Agreement, including, but not limited to any obligations during the warranty period and any extensions to the period. The security shall be returned to the Supplier no later than thirty (30) Days after its expiration. d) The security shall be reduced: i. pro rata by the portion of the Contract Price payable for any Subsystem(s) that has achieved Operational Acceptance, if permitted by the Contract Agreement, on the date of such Operational Acceptance; or ii. by the amount specified in the SCC, to reflect the Operational Acceptance of the entire System, on the date of such Operational Acceptance, so that the reduced security would only cover the remaining warranty obligations of the Supplier.
14	Taxes and Duties	14.1 If any tax exemptions, reductions, allowances, or privileges may be available to the Supplier in Pakistan, NBP shall use its best efforts to enable the Supplier to benefit from any such tax savings to the maximum allowable extent. 14.2 For the purpose of the Contract Agreement, it is agreed that the Contract Price specified in the Contract Agreement is based on the taxes, duties, levies, and charges prevailing at the date twenty-eight (28) Days prior to the date of bid submission in Pakistan (also called "Tax" in this GCC clause 14.4). If any Tax rates are increased or decreased, a new Tax is introduced, an existing Tax is abolished, or any change in interpretation or application of any Tax occurs in the course of the performance of the Contract Agreement, which was or will be assessed on the Supplier, its Subcontractors, or their employees in connection with the performance of the Contract Agreement, the parties shall come to an equitable understanding for payment of such taxes.

D. Intellectual Property

15	Copyright	15.1 The Intellectual Property Rights in all Standard Software and Standard Materials, Stationary/Cards shall remain vested in the owner of such rights. 15.2 NBP agrees to restrict the use, copying, or duplication of the Standard Software and Standard Materials Following GCC clause 16, except that additional copies of Standard Materials may be made by NBP for use within the scope of the project of which the System is a part, in the event that the Supplier does not deliver copies within thirty (30) Days from receipt of a request for such Standard Materials. 15.3 NBP's contractual rights to use the Standard Software or elements of the Standard Software may not be assigned, licensed, or otherwise transferred voluntarily except Following the relevant license agreement or as may be otherwise specified in the SCC. 15.4 NBP's and Supplier's rights and obligations with respect to Custom Software or elements of the Custom Software, including any license agreements, and 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 the Contract Agreement or on the creation of the rights (if later than the date of the Contract Agreement), vest in NBP. The Supplier shall perform and execute or arrange for the performance and execution of each necessary act, document, and thing that NBP may consider necessary or desirable to perfect the right, title, and

		interest of NBP in and to those rights. In respect of such Custom Software and Custom Materials, the Supplier shall ensure that the holder of any right in such an item does not assert it, and the Supplier shall, if requested to do so by NBP and where permitted by applicable law, ensure that the holder of such a right waives it. 15.5 The parties shall enter into such (if any) escrow arrangements in relation to the source code to some or all of the Software as specified in the SCC and Following the SCC or as specified in the Contract Agreement and if required execute a separate escrow agreement.
16	Software License Agreements	16.1 Except to the extent that the Intellectual Property Rights in the Software vest in NBP, the Supplier hereby grants to NBP a license to access and use the Software, including all inventions, designs, and marks embodied in the Software (if provided to NBP under the Contract Agreement). a) Such license to access and use the Software shall be: i) Exclusive. ii) fully paid up and irrevocable (except that it shall terminate if the Contract Agreement terminates under GCC clauses 41.1 or 41.3). iii) valid throughout the territory of Pakistan (or such other territory as specified in the SCC and the Contract Agreement); 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 computer(s) 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 the other computers to the extent necessary to that access. iv) reproduced for safekeeping or backup purposes; customized, adapted, or combined with other computer software for use by NBP, provided that derivative software incorporating any substantial part of the delivered, restricted Software shall be subject to the same restrictions as are outlined in the Contract Agreement. v) as specified in the SCC, disclosed to, and reproduced for use by, support service suppliers and their subcontractors, (and NBP may sublicense such persons to use and copy for use the Software) to the extent reasonably necessary for the performance of their support service contracts, subject to

		the same restrictions as are outlined in this Contract Agreement; and vi) disclosed to, and reproduced for use by, NBP and by such other persons as are specified in the SCC (and NBP may sublicense such persons to use and copy for use the Software), subject to the same restrictions as are outlined in the Contract Agreement. 16.2 The Standard Software may be subject to audit by the Supplier Following the terms specified in the SCC to verify compliance with the above license agreements.
17	Confidential Information	17.1 Unless otherwise specified in the SCC, NBP and the Supplier ("the Receiving Party") shall each keep confidential and shall not, without the written consent of the other party to the Contract Agreement ("the Disclosing Party"), divulge to any third party any documents, data, or other information of a confidential nature ("Confidential Information"): a) furnished directly or indirectly by the Disclosing Party in connection with this Contract; or b) where the Supplier is the Receiving Party, generated by the Supplier in the course of the performance of its obligations under the Contract and relating to the businesses, finances, suppliers, employees, or other contacts of NBP or NBP's use of the System, c) whether such information has been furnished or generated prior to, during, or following the termination of the Contract ("Confidential Information"). 17.2 Notwithstanding the above: a) the Supplier may furnish to its Subcontractor Confidential Information of NBP to the extent reasonably required for the Subcontractor to perform its work under the Contract; and b) NBP 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, c) 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 17 as if that person were party to the Contract Agreement in place of the Receiving Party. 17.3 NBP 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 NBP's prior written consent, use any Confidential Information received from NBP for any purpose other than those that are required for the performance of the Contract Agreement. 17.4 The obligation of a party under GCC clauses 17.1, 17.2, and 17.3 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. 17.5 The above provisions of this GCC clause 17 shall not in any way modify any undertaking confidentiality given by either of the parties to the Contract Agreement before the date of the Contract Agreement in respect of the System or any part thereof. 17.6 The provisions of this GCC clause 17 shall survive the termination, for whatever reason, of the Contract Agreement for three (3) Years or such longer period as may be specified in the SCC or the Contract Agreement.

E. Supply, Installation, Testing, Commissioning and Acceptance of the System

18	Representatives	18.1 Project Manager (Certified): a) If the Project Manager is not named in the Contract Agreement, then NBP shall appoint and notify the Supplier in writing of the name of the Project Manager within the period specified in the Contract Agreement or as mutually agreed. The terms and conditions of appointment shall be specified in the Contract Agreement. The Project Manager shall have the authority to represent NBP on all day-to-day matters relating to the System or arising from the Contract Agreement. All notices, instructions, orders, certificates, approvals, and all other communications under the Contract Agreement shall be given by the Project Manager, except as otherwise provided for in the Contract Agreement. b) All notices, instructions, information, and other communications given by the Supplier to NBP under the Contract Agreement shall be given to the Project Manager, except as otherwise provided for in the Contract Agreement. 18.2 Supplier’s Representative: a) If the Supplier’s Representative is not named in the Contract Agreement, then the Supplier shall appoint the Supplier’s Representative within the period specified in the Contract Agreement or as mutually agreed. The terms and conditions of appointment shall be specified in the Contract Agreement. The Supplier’s Representative shall have the authority to represent the Supplier on all day-to-day matters relating to the System or arising from the Contract Agreement. b) All notices, instructions, orders, certificates, approvals, and all other communications under the Contract Agreement shall be given by the Supplier’s Representative, except as otherwise provided for in the Contract Agreement. c) The Supplier shall not revoke the appointment of the Supplier’s Representative without NBP’s prior written consent, which shall not be unreasonably withheld. If NBP consents to such an action, the Supplier shall appoint another person of equal or superior qualifications as the Supplier’s Representative. d) The Supplier’s Representative and staff are obliged to work closely with NBP’s Project Manager and staff, act within their authority, and abide by directives issued by NBP that are consistent with the terms of the Contract Agreement. The Supplier’s Representative is responsible for managing the activities of its personnel and any subcontracted personnel.

		18.3 Objections and Removals: a) NBP may, by notice to the Supplier, object to any representative or person employed by the Supplier in the execution of the Contract Agreement who, in the reasonable opinion of NBP, may have behaved inappropriately, been incompetent, or negligent. NBP shall provide evidence of the same, whereupon the Supplier shall remove such person from work on the System. b) If any representative or person employed by the Supplier is removed Following the GCC and the Contract Agreement, the Supplier shall, where required, promptly appoint a replacement.
19	Project Plan	19.1 In close cooperation with NBP 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 Agreement. The contents of the Project Plan shall be as specified in the SCC and/or Technical Requirements. 19.2 The Supplier shall formally present the Project Plan to NBP Following the procedure specified in the SCC. 19.3 If required, the impact on the Implementation Schedule of modifications agreed upon during the finalization of the Project Plan shall be incorporated in the Contract by amendment, Following GCC clauses 39 and 40. 19.4 The Supplier shall undertake to supply, install, test, and commission the System Following the Finalized Project Plan as agreed to by NBP and as per the Contract Agreement. 19.5 The progress and other reports specified in the SCC shall be prepared by the Supplier and submitted to NBP in the format and frequency specified in the Technical Requirements.
20	Subcontracting	20.1 The Supplier shall prepare a list of Subcontractors it considers necessary for the project, and which are, in the opinion of the Supplier, qualified to perform the duties entrusted to them by the Supplier. The appointment of the Subcontractors by the Supplier shall be subject to the approval of NBP. A list of the Subcontractors and the items for which they may be hired shall be annexed to the Contract Agreement. 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 NBP for its approval in sufficient time so as not to impede the progress of work on the System. NBP shall not withhold such approval unreasonably. Approval by NBP of a Subcontractor shall not relieve the Supplier of any of its obligations, duties, or responsibilities under the Contract Agreement. 20.2 The Supplier may, at its discretion, select and employ Subcontractors for such critical items from the Subcontractors listed pursuant to GCC clause 20.1. If the Supplier wishes to employ a Subcontractor not so listed, or subcontract an item not so listed, it must seek NBP's prior approval under GCC clause 20.3. 20.3 For items for which pre-approved Subcontractor lists have not been specified in the Contract Agreement, the Supplier may employ such Subcontractors as it may select, provided, it obtains NBP's written consent to such appointment.
21	Design and Engineering	21.1 Technical Specifications and Drawings: a) The Supplier shall execute the basic and detailed design and implementation activities necessary for successful installation of the System in compliance with the provisions of amongst others or provision of any material i.e.,

Plastic/Inventory, the Technical Requirements, and the Contract Agreement or, where not so specified, Following good industry practice.

b) The Supplier shall be responsible for any discrepancies, errors, or omissions in the specifications, drawings, and other technical documents that it has prepared, whether such specifications, drawings, and other documents have been approved by the Project Manager or not, provided that such discrepancies, errors, or omissions are not based on inaccurate information furnished in writing to the Supplier by or on behalf of NBP.

c) The Supplier shall be entitled to disclaim responsibility for any design, data, drawing, specification, standards, or another document, or any modification of such design, drawings, specification, or other documents provided or designated by or on behalf of the NBP, by giving a notice of such disclaimer to the Project/Product Manager.

21.2 Codes and Standards

a) Wherever references are made in the Contract Agreement or the GCC and the SCC to codes and standards Following which the Contract Agreement shall be performed, the edition or the revised version of such codes and standards current at the date twenty-eight (28) Days prior to the date of bid submission shall apply unless otherwise specified in the SCC. During the performance of the Contract Agreement, any changes in such codes and standards shall be applied after approval by the NBP and shall be treated Following GCC clause 39.3.

21.3 Approval/Review of Technical Documents by the Project Manager.

a) The Supplier shall prepare and furnish to the Project Manager the documents as specified in the SCC for the Project Manager's approval or review. Any part of the System covered by or related to the documents to be approved by the Project Manager shall be executed only after the Project Manager approves these documents. GCC clauses 21.3.2 through 21.3.7 shall apply to those documents requiring the Project Manager's approval, but not to those furnished to the Project Manager for review only.

b) Any document requiring the Project Manager's approval Following GCC clause 21.3.1, shall be submitted to the Project Manager. The Project Manager shall either return one copy of the document to the Supplier with its approval endorsed on the document or shall notify the Supplier in writing of its disapproval of the document and the reasons for disapproval and the modifications that the Project Manager proposes.

21.4 The Project/Product Manager shall not disapprove of any document except on the grounds that the document does not comply with some specified provision of the Technical Requirements, the Contract Agreement, or that it is contrary to good industry practice.

21.5 If the Project/Product Manager disapproves the document, the Supplier shall modify the document and resubmit it for the Project Manager's approval Following GCC clause 21.3.2. If the Project Manager approves the document subject to modification(s), the Supplier shall make the required modification(s), and the document shall then be deemed to have been approved, subject to GCC clause 21.3.5. The procedure set out in GCC clauses 21.3.2 through 21.3.4 shall be repeated, as appropriate, until the Project Manager approves such documents.

		21.6 If any dispute or difference occurs between NBP and the Supplier in connection with or arising out of the disapproval by the Project Manager of any document and/or any modification(s) to a document that cannot be settled between the parties within a reasonable period, then, the matter shall be referred for resolution in the manner provided in the Contract Agreement. 21.7 The Supplier shall not depart from any approved document unless the Supplier has first submitted to the Project Manager an amended document and obtained the Project Manager's approval of the document, pursuant to the provisions of this GCC clause 21.3. If the Project Manager requests any change in any already approved document and/or in any document based on such an approved document, the provisions of GCC clause 39 (Changes to the System) shall apply to such request.
22	Procurement Delivery and Transport	22.1 Subject to GCC clause 14.2, 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. 22.2 Delivery of the Information Technologies, Materials, and other Goods shall be made by the Supplier Following the Technical Requirements. (If applicable) 22.3 Early or partial deliveries require the explicit written consent of NBP, which shall not be unreasonably withheld. 22.4 Transportation: a) 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 NBP's instructions given to the Supplier and with the manufacturers' instructions. b) 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 terms. c) 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. 22.5 Unless otherwise specified in the SCC, the Supplier will provide NBP with shipping and other documents, as specified below: 22.5.1 For Goods supplied from outside Pakistan: Upon shipment, the Supplier shall notify NBP, 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 NBP 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 Pakistan and at the site. 22.5.2 For Goods supplied locally (i.e., from within the Pakistan): a) Upon shipment, the Supplier shall notify NBP by facsimile, electronic mail, or EDI with the full details of the shipment. The Supplier shall promptly send the following documents to the NBP by courier: b) two copies of the Supplier's invoice showing the Goods' description, quantity, unit price, and total amount. c) delivery note, railway receipt, or truck receipt. d) certificate of insurance. e) Estimated time of arrival at the site. 22.6 Customs Clearance a) Unless specified otherwise, the Supplier will bear responsibility for, and cost of, customs clearance into Pakistan in accordance with the particular conditions used for Goods supplied from outside Pakistan. b) At the request of the Supplier, NBP will make available a representative or agent during the process of customs clearance in Pakistan for Goods supplied from outside Pakistan. In the event of delays in customs clearance that are not the fault of the Supplier, the Supplier shall be entitled to an extension in the time for achieving Operational Acceptance, pursuant to GCC clause 40;
23	Product Upgrades	23.1 At any point during the performance of the Contract Agreement, should technical upgradation be introduced by the Supplier for the technical solution originally offered by the Supplier in its bid and still to be delivered, the Supplier shall be obligated to offer to NBP the latest versions of the available technical solutions having equal or better performance or functionality at the same or lesser unit prices, pursuant to GCC clause 39 (Changes to the System). 23.2 At any point during the performance of the Contract Agreement for technical solutions yet to be delivered, the Supplier will also pass on to NBP any cost reductions and additional and/or improved support and facilities that it offers to other clients of the Supplier in Pakistan, pursuant to GCC clause 39 (Changes to the System). 23.3 During the performance of the Contract Agreement, the Supplier shall offer to NBP all new versions, releases, and updates of the offered technical solution, 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 Pakistan, and no later than twelve (12) Months after they are released in the country of origin. In all such cases, the costs shall be decided by mutual consent or Following the Contract Agreement or any other related agreement between the parties. 23.4 During the Warranty Period, unless otherwise specified in the SCC, the Supplier will provide, at no additional cost to NBP, all new versions, releases, and updates for the offered technical solution to be used in the System, within thirty (30) Days of their availability from the Supplier to other clients of the Supplier in Pakistan, and no later than twelve (12) Months after they are released in the country of origin of the Software. 23.5 NBP shall introduce all new versions, releases, or updates of the offered technical

		solution within the time agreed in the Contract Agreement. The receipt of upgraded technical equipment should not adversely affect System operation or performance or require extensive reworking of the System. In cases where the new version, release, or update adversely affects System operation or performance or requires extensive reworking of the System, the Supplier shall continue to support and maintain the technical equipment previously in operation for as long as necessary to allow the introduction of the new upgrades. NBP shall use all reasonable endeavors to implement any new upgrades as soon as practicable.
24	Implementation, Installation, and Other Services	24.1 The Supplier shall provide all Services specified in the Contract Agreement and the Finalized Project Plan Following the highest standards of professional competence and integrity. 24.2 Prices charged by the Supplier for Services, if not included in the Contract Agreement, shall be agreed upon in advance by the parties (including, but not restricted to, any prices submitted by the Supplier in the Bid) and shall not exceed the prevailing rates charged by the Supplier to other clients in Pakistan for similar services.
25	Inspection and Test	25.1 NBP or its representative shall have the right to inspect and/or test any components of the offered technical solution, material, or stationary, as specified in the Technical Requirements, to confirm their good working order/quality and/or conformity to the Contract Agreement at the point of delivery and/or at the Project/Production Site. 25.2 NBP and the Project/Product Manager or their designated representatives shall be entitled to attend any such inspections and/or tests of the components, provided that NBP shall bear all costs and expenses incurred in connection with such attendance, including but not limited to all inspection agent fees, travel, and related expenses. 25.3 Should the inspected or tested components fail to conform to the Contract Agreement NBP may reject the component(s), and the Supplier shall either replace the rejected component(s) or make alterations as necessary so that it meets the Contract Agreement requirements free of cost to the NBP. 25.4 The Project Manager may require the Supplier to carry out any inspection and/or test not specified in the Contract Agreement, provided that the Supplier's reasonable costs and expenses incurred in carrying out such inspection and/or test shall be reimbursable by NBP to the Supplier, provided that the tests are not required due to any breach of the Contract Agreement and the Technical Requirements by the Supplier. Further, if such inspection and/or test impede the progress of work on networking and/or the Supplier's performance of its other obligations under the Contract Agreement, the due allowance will be made in respect of the time for achieving Operational Acceptance and the other obligations so affected at the discretion of NBP. 25.5 If any dispute or difference of opinion shall arise between the parties in connection with or caused by an inspection and/or with regard to any hardware devices or technical equipment to be incorporated in the network that cannot be settled amicably between the parties within a reasonable period, either party may invoke the process pursuant to GCC clause 6 (Settlement of Disputes).

26	Installation of the System	26.1 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 Following the Technical Requirements, the SCC and the Finalized Project Plan, the Supplier shall notify NBP of the same in writing as provided/mentioned in the agreement. 26.2 The Project Manager shall after receipt of the Supplier's notice under GCC clause 26.1, either issue an Installation certificate, stating that the hardware devices or technical equipment (if acceptance by major component or Subsystem is specified in the Contract), has achieved Installation by the date of the Supplier's notice under GCC clause 26.1, or notify the Supplier in writing of any defects and/or deficiencies, including, but not limited to, defects or deficiencies in the interoperability of the various hardware devices or technical equipment making up the network. 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 network and, when in the Supplier's opinion, the network is ready for Commissioning and Operational Acceptance Testing, notify the NBP in writing, Following GCC clause 26.1. The procedure set out in this GCC clause 26.2 shall be repeated, as necessary, until an Installation certificate is issued.
27	Commissioning and Operational Acceptance	27.1 Commissioning: 27.1.1 Commissioning of the network (or technical equipment if specified in the Contract Agreement) shall be commenced by the Supplier: a) immediately after the Installation certificate is issued by the Project Manager, pursuant to GCC clause 26.2; or b) as otherwise specified in the Technical Requirement or the Finalized Project Plan. 27.1.2 NBP shall supply the operating and technical materials and information reasonably required to enable the Supplier to carry out its obligations with respect to Commissioning. 27.2 Operational Acceptance Tests 27.2.1 The Operational Acceptance Tests (and repeats of such tests) shall be the joint responsibility of NBP and the Supplier and shall be conducted during the Commissioning of the network unless specified otherwise in the Contract Agreement. The Operational Acceptance Tests shall be carried out, to ascertain whether the network (or technical equipment or hardware devices) 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 Finalized Project Plan. 27.2.2 At NBP's discretion, Operational Acceptance Tests may also be performed on replacement software, upgrades and new version releases, and Goods that are added or field-modified after Operational Acceptance of the System. 27.3 Operational Acceptance:

		27.3.1 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 Finalized Project Plan have been completed; or b) After NBP has put the network into operation or use for sixty (60) consecutive Days. If the System is put into production or used in this manner, the Supplier shall notify NBP and document such use. 27.4 At any time after any of the events set out in GCC clause 27.3.1 have occurred, the Supplier may give notice to the Project Manager requesting the issuance of an Operational Acceptance certificate. 27.5 After consultation with NBP, 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. 27.6 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 NBP, and NBP, with the full cooperation of the Supplier, shall use all reasonable endeavors to promptly carry out retesting of the network or technical equipment or hardware devices. Upon the successful conclusion of the Operational Acceptance Tests, the Supplier shall notify NBP of its request for Operational Acceptance certification, Following GCC clause 27.3.3. NBP shall then issue the Operational Acceptance certification to the Supplier Following GCC clause 27.3.3 (a) or shall notify the Supplier of further defects, deficiencies, or other reasons for the failure of the Operational Acceptance Test. 27.7 The procedure set out in this GCC clause 27.3.4 shall be repeated, as necessary, until an Operational Acceptance certificate is issued. 27.7.1 If the technical solution provided fails to pass the Operational Acceptance Test(s) Following GCC clause 27.2, then NBP may consider terminating the Contract, according to GCC clause 41.2.2.

F. Guarantees and Liabilities

28	Operational Acceptance Time Guarantee	28.1 The Supplier guarantees that it shall supply, and complete the Installation and Commissioning of the System (or Subsystems if specified in the Contract), material/Plastic and achieve Operational Acceptance of the System (or Subsystems, if specified in the Contract) within the periods specified in the implementation schedule in the Technical Requirements section and/or the Finalized Project Plan pursuant to GCC clause 8.2, or within such extended time to which the Supplier shall be entitled under GCC clause 40 (Extension of Time for Achieving Operational Acceptance). 28.2 If the Supplier fails to supply standard material/stationary, install, commission, and achieve Operational Acceptance of the System (or Subsystems if specified in the Contract Agreement) within the time for achieving Operational Acceptance specified in the implementation schedule in the Technical Requirement or the Finalized Project Plan, or any extension of the time for achieving Operational Acceptance previously granted under GCC clause 40 (Extension of Time for Achieving Operational Acceptance), the Supplier shall pay to NBP, liquidated damages at the rate specified in the SCC as a percentage of the Contract Price, or the relevant part of the Contract Price if a Subsystem has not achieved Operational Acceptance. 28.3 The aggregate amount of such liquidated damages shall not exceed the amount specified in the Contract Agreement (if any). Once the maximum (if any) is reached, NBP may consider termination of the Contract Agreement, pursuant to GCC clause 41.2.2. 28.4 Unless otherwise specified in the SCC or the Contract Agreement, liquidated damages payable under GCC clause 28.2 shall only apply to the failure to achieve Operational Acceptance of the System (and Subsystems) as specified in the implementation schedule in the Technical Requirements and/or Finalized Project Plan. This clause 28.3 shall not limit any other rights or remedies that NBP may have under the Contract Agreement for other delays. 28.5 The payment of liquidated damages shall not in any way relieve the Supplier from any of its obligations to complete the System or from any of its other obligations and liabilities under the Contract Agreement.
29	Defect Liability	29.1 The Supplier warrants that the provided technical solution along with the materials, and other Goods supplied, and Services provided, shall be free from defects in design, engineering, Materials, and workmanship that prevent the System and/or any of its components from fulfilling the Technical Requirements or that limits, in a material fashion, the performance, reliability, or extensibility of the System and/or Subsystems. Exceptions and/or limitations, if any, to this warranty concerning hardware or technical equipment, shall be as specified in the SCC. Commercial warranty provisions of products supplied under the Contract Agreement shall apply to the extent that they do not conflict with the provisions of this Contract Agreement. 29.2 The Supplier also warrants that the Information Technologies, Materials, and other Goods supplied under the Contract Agreement are new, unused, and incorporate all recent improvements in design that materially affect the System's or Subsystem's ability to fulfill the Technical Requirements. 29.3 In addition, the Supplier warrants that:

a) all hardware components to be incorporated into the System form part of the Supplier's and/or Subcontractor's current product lines,

b) they have been previously released to the market, and

c) those specific items identified in the SCC (if any) have been in the market for at least the minimum periods specified in the SCC.

29.4 The 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 Agreement) and shall extend for the length of time specified in the SCC and the Contract Agreement.

29.5 If during the Warranty Period, any defect as described in GCC clause 29.1 should be found in the design, engineering, Materials, and workmanship of the provided technical solution and other hardware supplied or of the Services provided by the Supplier, the Supplier shall promptly, in consultation and agreement with NBP regarding appropriate remedying of the defects, and at its sole cost, repair, replace, or otherwise make good, such defect as well as any damage to the System caused by such defect. Any defective technical solution or other hardware that has/have been replaced by the Supplier shall remain the property of the Supplier.

29.6 The Supplier shall not be responsible for the repair, replacement, or making good of any defect, or of any damage to the System arising out of or resulting from any of the following causes:

a) Improper operation or maintenance of the System by NBP.

b) Normal wear and tear.

c) Use of the System with items not supplied by the Supplier, unless otherwise identified in the Technical Requirements, or approved by the Supplier; or

d) Modifications made to the System by NBP, or a third party, not approved by the Supplier.

29.7 The Supplier's obligations under this GCC clause 29 shall not apply to:

a) Any materials that are normally consumed in operation or have a normal life shorter than the Warranty Period; or

b) Any designs, specifications, or other data designed, supplied, or specified by or on behalf of NBP or any matters for which the Supplier has expressly disclaimed responsibility, Following GCC clause 21.1.2 and in the Contract Agreement.

29.8 NBP shall promptly notify the Supplier of a defect following the discovery of such defect, stating the nature of any such defect together with all available evidence. NBP shall afford all reasonable opportunities for the Supplier to inspect any such defect. The NBP shall afford the Supplier all necessary access to the System and the Project Site to enable the Supplier to perform its obligations under this GCC clause 29.

29.9 The Supplier may, with NBP's consent, remove from the Project Site, any technical solution and other hardware or technical equipment that are defective, if the nature of the defect, and/or any damage to the System caused by the defect, is such that repairs cannot be expeditiously carried out at the Project Site. If the repair, replacement, or making good is of such a character that it may affect the efficiency of the System, NBP may give the Supplier notice requiring tests of the

		defective part to be made by the Supplier immediately upon completion of such remedial work, whereupon the Supplier shall carry out such tests. 29.10 If such part fails the tests, the Supplier shall carry out further repair, replacement, or making good (as the case may be) until that part of the System passes such tests. The tests shall be agreed upon by the NBP and the Supplier. 29.11 If the Supplier fails to commence the work necessary to remedy such defect or any damage to the System caused by such defect within the time period specified in the SCC, NBP may, following notice to the Supplier, proceed to do such work or contract a third party (or parties) to do such work, and the reasonable costs incurred by NBP in connection with such work shall be paid to NBP by the Supplier or may be deducted by NBP from any due payment to the Supplier or claimed under the Performance Security. 29.12 If the System or Subsystem cannot be used by reason of such defect and/or making good of such defect, the Warranty Period for the System shall be extended by a period equal to the period during which the System or Subsystem could not be used by NBP because of such defect and/or making good of such defect. 29.13 Items substituted for defective parts of the System during the Warranty Period shall be covered by the defect liability warranty for the remainder of the Warranty Period applicable for the part replaced or three (3) Months, whichever is greater. At the request of NBP and without prejudice to any other rights and remedies that NBP may have against the Supplier under the Contract Agreement, the Supplier will offer all possible assistance to NBP to seek warranty services or remedial action from any subcontracted third-party producers or licensor of Goods included in the System, including without limitation assignment or transfer in favor of NBP of the benefit of any warranties given by such producers or licensors to the Supplier. 29.14 The Supplier guarantees that once the Operational Acceptance Certificate(s) has been issued, the System represents a complete, integrated solution to NBP's requirements set forth in the Technical Requirements and it conforms to all other aspects of the Contract Agreement. The Supplier acknowledges that GCC clause 27 regarding Commissioning and Operational Acceptance governs how technical conformance of the System to the Contract Agreement requirements will be determined. 29.15 If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract Agreement, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify NBP upon completion of the necessary changes, modifications, and/or additions and shall request NBP to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance. 29.16 If the System (or Subsystem(s)) fails to achieve Operational Acceptance, NBP may consider termination of the Contract Agreement, pursuant to GCC clause 41.2.2, and forfeiture of the Supplier's performance security as compensation for the extra costs and delays likely to result from this failure.

30	Functional Guarantee	30.1 The Supplier guarantees that once the Operational Acceptance Certificate(s) has been issued, the System/supply of material to NBP's requirements set forth in the Technical Requirements conforms to all other aspects of the Contract Agreement. The Supplier acknowledges that GCC clause 27 regarding Commissioning and Operational Acceptance governs how technical conformance of the System, and Material to the Contract Agreement requirements will be determined. 30.2 If, for reasons attributable to the Supplier, the System does not conform to the Technical Requirements or does not conform to all other aspects of the Contract Agreement, the Supplier shall at its cost and expense make such changes, modifications, and/or additions to the System as may be necessary to conform to the Technical Requirements and meet all functional and performance standards. The Supplier shall notify NBP upon completion of the necessary changes, modifications, and/or additions and shall request NBP to repeat the Operational Acceptance Tests until the System achieves Operational Acceptance. 30.3 If the System (or Subsystem(s)) fails to achieve Operational Acceptance, NBP may consider termination of the Contract Agreement, pursuant to GCC clause 41.2.2, and forfeiture of the Supplier's performance security as compensation for the extra costs and delays likely to result from this failure.
31	Intellectual Property Rights Warranty	31.1 The Supplier hereby represents and warrants that: a) The System. Material, and inventory as supplied, installed, tested, and accepted. b) Use of the System Following the Contract Agreement; and c) Copying of the Software and Materials provided to NBP Following the Contract Agreement; do not and will not infringe any Intellectual Property Rights held by any third party, and that it has all necessary rights or at its sole expense shall have secured in writing all transfers of rights and other consents necessary to make the assignments, licenses, and other transfers of Intellectual Property Rights and the warranties set forth in the Contract Agreement, and for NBP to own or exercise all Intellectual Property Rights as provided in the Contract Agreement. Without limitation, the Supplier shall secure all necessary written agreements, consents, and transfers of rights from its employees and other persons or entities whose services are used for the development of the System.
32	Intellectual Property Rights Indemnity	32.1 The Supplier shall indemnify and hold harmless NBP and its employees and officers from and against any or all losses, liabilities, and costs (including losses, liabilities, and costs incurred in defending a claim alleging such a liability), that NBP or its employees or officers may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights because of: a) installation of the System by the Supplier or the use of the System, including the Materials, in the country where the Project Site is located. b) copying of the Software and Materials provided by the Supplier Following the Contract Agreement or any agreement with the Supplier relating to licensing; 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 NBP 's

breach of GCC clause 32.2.

32.2 Such indemnity shall not cover any use of the System, including the Materials, other than for the purpose reflected in the Contract Agreement, 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.

32.3 Such indemnities shall also not apply if any claim of infringement:

a) is a direct result of a design mandated by NBP's Technical Requirements and the possibility of such infringement has been notified in writing to NBP in the Supplier's Bid; or

b) Results from the alteration of the System, including the Materials without authorization of the Supplier, by NBP or any persons other than the Supplier or a person authorized by the Supplier.

32.4 If any proceedings are brought or any claim is made against NBP arising out of the matters referred to in GCC clause 32.1, NBP shall promptly notify the Supplier of such proceedings or claims, and the Supplier may at its own expense and in NBP's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

32.5 If the Supplier fails to notify its intention to conduct any such proceedings or claims to NBP within twenty-eight (28) Days after receipt of such notice, then NBP shall be free to conduct the same on its own behalf. Unless the Supplier fails to notify NBP within twenty-eight (28) Days, NBP shall make no admission that may be prejudicial to the defense of any such proceedings or claim. NBP shall, at the Supplier's request, provide all available assistance to the Supplier in conducting such proceedings or claims and shall be reimbursed by the Supplier for all reasonable expenses incurred in doing so.

32.6 NBP shall indemnify and hold harmless the Supplier and its employees, officers, and Subcontractors 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 Supplier may suffer as a result of any infringement or alleged infringement of any Intellectual Property Rights arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided to the Supplier in connection with the Contract Agreement by NBP or any persons (other than the Supplier) contracted by NBP, except to the extent that such losses, liabilities, and costs arise as a result of the Supplier's breach of GCC clause 32.8.

32.7 Such indemnity shall not cover any use of the design, data, drawing, specification, or other documents or materials, other than for the purpose indicated by or to be reasonably inferred from the Contract Agreement, or any infringement resulting from the use of the design, data, drawing, specification, or other documents or materials, or any products produced thereby, in association or in combination with any other Goods or Services not provided by NBP or any other person contacted by NBP, where the infringement arises because of such association or combination and not because of the use of the design, data, drawing, specification, or other documents or materials in its own right.

32.8 Such indemnities shall also not apply:

		a) if any claim of infringement is asserted by a parent, subsidiary, or affiliate of the Supplier's organization. b) to the extent that any claim of infringement caused by the alteration by the Supplier, or any persons contracted by the Supplier, of the design, data, drawing, specification, or other documents or materials provided to the Supplier by NBP, or any persons contracted by NBP. 32.9 If any proceedings are brought or any claim is made against the Supplier arising out of the matters referred to in GCC clause 32.5, the Supplier shall promptly notify NBP about such proceedings or claims, and NBP may at its own expense and in the Supplier's, name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If NBP fails to notify the Supplier within twenty-eight (28) Days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Supplier shall be free to conduct the same on its own behalf. Unless NBP has failed to notify the Supplier within twenty-eight (28) Days, the Supplier shall make no admission that may be prejudicial to the defense of any such proceedings or claim. The Supplier shall, at NBP's request, afford all available assistance to NBP in conducting such proceedings or claims and shall be reimbursed by the NBP for all reasonable expenses incurred in so doing.
33	Limitation of Liability	33.1 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 NBP, 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 NBP; and b) the aggregate liability of the Supplier to NBP, whether under the Contract, in tort or otherwise, shall not exceed the amount specified in the Contract Agreement (if any), provided that this limitation shall not apply to any obligation of the Supplier to indemnify NBP with respect to intellectual property rights infringement.

G. Risk Distribution

34	Transfer of Ownership	34.1 Unless provided otherwise in the Contract Agreement, with the exception of Software and Materials, the ownership of the technical solution and other Goods shall be transferred to NBP at the time of Delivery or otherwise under terms that may be agreed upon and specified in the Contract Agreement. 34.2 The ownership and terms of usage of the Software and Materials supplied under the Contract shall be governed by GCC clause 15 (Copyright) and any elaboration in the Technical Requirements. 34.3 Unless provided otherwise in the Contract Agreement the ownership of the Supplier's Equipment used by the Supplier and its Subcontractors in connection with the Contract Agreement shall remain with the Supplier or its Subcontractors.

35	Care of the System	35.1 NBP shall become responsible for the care and custody of the System or Subsystems, material, and Inventory upon their Delivery. NBP shall make good at its own cost any loss or damage that may occur to the System or Subsystems due to any reason from the date of Delivery until the date of Operational Acceptance of the System or Subsystems, pursuant to GCC clause 27 (Commissioning and Operational Acceptance), except for such loss or damage arising from acts or omissions of the Supplier, its employees, or Subcontractors. 35.2 NBP shall pay to the Supplier all sums payable in respect of the System or Subsystems that have achieved Operational Acceptance, notwithstanding that the same be lost, destroyed, or damaged. If NBP requests the Supplier in writing to make good any loss or damage to the System thereby occasioned, the Supplier shall make good the same at NBP's cost Following GCC clause 39. If NBP does not request the Supplier in writing to make good any loss or damage to the System thereby occasioned, 35.3 NBP shall either request a change Following GCC clause 39, excluding the performance of that part of the System thereby lost, destroyed, or damaged, or, where the loss or damage affects a substantial part of the System, NBP shall terminate the Contract Agreement. 35.4 NBP shall be liable for any loss of or damage to the Supplier's Equipment which (if) NBP has authorized to locate within NBP's premises for use in fulfillment of the Supplier's obligations under the Contract Agreement, except where such loss or damage arises from acts or omissions of the Supplier, its employees, or Subcontractors.
36	Loss of or Damage to Property; Accident or Injury to Workers; Indemnification	36.1 The Supplier and each and every Subcontractor shall abide by the job safety, insurance, customs, and immigration measures prevalent and laws in force in Pakistan. Subject to GCC clause 36.3, the Supplier shall indemnify and hold harmless NBP 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 NBP or its employees or officers may suffer as a result of the death or injury of any person or loss of or damage to any property (other than the System, whether accepted or not) arising in connection with the supply, Installation, testing, and Commissioning of the System and by reason of the negligence of the Supplier or its Subcontractors, or their employees, officers or agents, except any injury, death, or property damage caused by the negligence of NBP, its contractors, employees, officers, or agents. 36.2 If any proceedings are brought or any claim is made against NBP that might subject the Supplier to liability under GCC clause 36.2, NBP shall promptly notify the Supplier of such proceedings or claims, and the Supplier may at its own expense and in NBP's name, conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim. If the Supplier fails to notify NBP within twenty-eight (28) Days after receipt of such notice that it intends to conduct any such proceedings or claim, then NBP shall be free to conduct the same on its own behalf. Unless the Supplier has failed to notify NBP within the twenty-eight (28) day period, NBP shall make no admission that may be prejudicial to the defense of any such proceedings or claim. NBP shall, at the Supplier's request, provide all available assistance to the Supplier in conducting such proceedings or claims and shall be reimbursed by the Supplier for all reasonable expenses incurred in so doing. 36.3 NBP shall take all reasonable measures to mitigate any loss or damage that has

		occurred.
37	Insurance	37.1 The Supplier shall at its expense take out and maintain in effect or cause to be taken out and maintained in effect, during the performance of the Contract Agreement, the insurance set forth below. The identity of the insurers and the form of the policies shall be subject to the approval of NBP, which approval shall not be withheld unreasonably. 37.2 Cargo Insurance During Transport: As applicable, 110 percent of the price of the technical solution or hardware or technical equipment and other Goods in a freely convertible currency, covering the Goods from physical loss or damage during shipment through receipt at the Project Site. 37.3 Installation "All Risks" Insurance: As applicable, 110 percent of the price of the technical solution or hardware or technical equipment and other Goods covering the Goods at the site from all risks of physical loss or damage (excluding perils commonly excluded under "all risks" insurance policies of this type by reputable insurers) occurring prior to Operational Acceptance of the System. 37.4 Third-Party Liability Insurance: On terms, as specified in the SCC, covering bodily injury or death suffered by third parties (including NBP's personnel) and loss of or damage to property (including NBP 's property and any Subsystems that have been accepted by NBP) occurring in connection with the supply and installation of the technical solution or hardware or technical equipment. 37.5 Automobile Liability Insurance: In accordance with the statutory requirements prevailing in Pakistan, covering the use of all vehicles used by the Supplier or its Subcontractors (whether or not owned by them) in connection with the performance of the Contract Agreement. 37.6 Other Insurance (if any), as specified in the SCC or the Contract Agreement 37.7 NBP shall be named as co-insured under all insurance policies taken out by the Supplier pursuant to GCC clause 37.1, except for the Third-Party Liability, and the Supplier's Subcontractors shall be named as co-insured (subject to the Subcontractors having an insurable interest) under all insurance policies taken out by the Supplier pursuant to GCC clause 37.1 except for Cargo Insurance During Transport. All insurers' rights of subrogation against such co-insured for losses or claims arising out of the performance of the Contract Agreement shall be waived under such policies. 37.8 The Supplier shall deliver to NBP certificates of insurance (or copies of the insurance policies) as evidence that the required policies are in full force and effect. 37.9 The Supplier shall ensure that, where applicable, its Subcontractor(s) shall take out and maintain in effect adequate insurance policies for their personnel and vehicles and work executed by them under the Contract Agreement, unless such Subcontractors are covered by the policies taken out by the Supplier. 37.10 If the Supplier fails to take out and/or maintain in effect the insurance referred to in GCC clause 37, NBP may take out and maintain in effect any such insurance and may from time to time deduct from any amount due the Supplier under the Contract Agreement, any premium that NBP shall have paid to the insurer or may otherwise recover such amount as a debt due from the Supplier. 37.11 Unless otherwise provided in the Contract Agreement, the Supplier shall prepare

		and conduct all and any claims made under the policies affected by it pursuant to this GCC clause and all money payable by any insurers shall be paid to the Supplier. NBP shall give the Supplier all such reasonable assistance as may be required by the Supplier in connection with any claim under the relevant insurance policies. With respect to insurance claims in which NBP's interest is involved, the Supplier shall not give any release or make any compromise with the insurer without the prior written consent of NBP. With respect to insurance claims in which the Supplier's interest is involved, NBP shall not give any release or make any compromise with the insurer without the prior written consent of the Supplier
38	Force Majeure	38.1 Force Majeure" shall mean any event beyond the reasonable control of NBP or of the Supplier, as the case may be, and which is unavoidable notwithstanding the reasonable care of the party affected and shall include, without limitation, the following: a) War, hostilities, warlike operations (whether a state of war is declared or not), invasion, the act of a foreign enemy, and civil war. b) Rebellion, revolution, insurrection, mutiny, usurpation of the civil or military government, conspiracy, riot, civil commotion, and terrorist acts. c) Confiscation, nationalization, mobilization, commandeering, or requisition by or under the order of any government or de jure or de facto authority or ruler, or any other act or failure to act, of any local state or national government authority. d) Epidemics, quarantine, and plague. e) Earthquakes, landslides, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricanes, storms, lightning, or other inclement weather conditions, nuclear and pressure waves, or other natural or physical disasters. 38.2 If either party is prevented, hindered, or delayed from performing any of its obligations under the Contract Agreement by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within fourteen (14) Days after the occurrence of such event. 38.3 The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract Agreement for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The time for achieving Operational Acceptance shall be extended Following GCC clause 40 (Extension of Time for Achieving Operational Acceptance). 38.4 The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract Agreement and to fulfill its or their obligations under the Contract Agreement but without prejudice to either party's right to terminate the Contract Agreement under GCC clause 38.6. 38.5 No delay or nonperformance by either party to this Contract Agreement caused by the occurrence of any event of Force Majeure shall: a) Constitute a default or breach of the Contract Agreement. b) Subject to GCC clauses 35.2, 38.3, and 38.4, give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance; if,

		and to the extent that, such delay or nonperformance is caused by the occurrence of an event of Force Majeure. 38.6 If the performance of the Contract Agreement is substantially prevented, hindered, or delayed for a single period of more than sixty (60) Days or an aggregate period of more than one hundred and twenty (120) Days on account of one or more events of Force Majeure during the time period covered by the Contract Agreement, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract Agreement by giving notice to the other. 38.7 In the event of termination pursuant to GCC clause 38.6, the rights and obligations of NBP and the Supplier shall be as specified in GCC clauses 41.1.2 and 41.1.3.

H. Change in Contract Elements

39	Changes to the System	39.1 Introducing a Change: a) Subject to GCC clauses 39.2.5 and 39.2.7, NBP shall have the right to propose, and subsequently require, the Project Manager to order the Supplier from time to time during the performance of the Contract Agreement to make any change, modification, addition, or deletion to, in, or from the System (interchangeably called "Change"), provided that such Change falls within the general scope of the System, does not constitute unrelated work, and is technically practicable, taking into account both the state of advancement of the System and the technical compatibility of the Change envisaged with the nature of the System as originally specified in the Contract Agreement. b) A Change may involve, but is not restricted to, the substitution of updated technical solutions and related Services Following GCC clause 23 (Product Upgrades). 39.1.2 The Supplier may, from time to time during its performance of the Contract Agreement propose to NBP (with a copy to the Project Manager) any Change that the Supplier considers necessary or desirable to improve the quality or efficiency of the System. The NBP may at its discretion approve or reject any Change proposed by the Supplier. 39.1.3 Notwithstanding GCC clauses 39.1.1 and 39.1.2, no change made necessary because of any default of the Supplier in the performance of its obligations under the Contract Agreement shall be deemed to be a Change, and such change shall not result in any adjustment of the time for Achieving Operational Acceptance. 39.1.4 The procedure on how to proceed with and execute Changes is specified in GCC clauses 39.2 and 39.3, and further details and sample forms are provided in the Sample Forms section in the Bidding Documents. 39.1.5 Moreover, NBP and the Supplier will agree, during the development of the Project Plan, to a date prior to the scheduled date for Operational Acceptance, after which the Technical Requirements for the System shall be "frozen." Any Change initiated after this time will be dealt with after Operational Acceptance. 39.2 Changes Originating from NBP: 39.2.1 If NBP proposes a Change pursuant to GCC clauses 39.1.1, it shall send to the

Supplier a "Request for Change Proposal," requiring the Supplier to prepare and furnish to the Project Manager as soon as reasonably practicable a "Change Proposal," which shall include the following:

a) Brief description of the Change.

b) Impact on the time for achieving Operational Acceptance.

c) The detailed estimated cost of the Change.

d) Effect on Functional Guarantees (if any).

e) Effect on any other provisions of the Contract Agreement.

39.2.2 Prior to preparing and submitting the "Change Proposal," the Supplier shall submit to the Project Manager a "Change Estimate Proposal," which shall be an estimate of the cost of preparing the Change Proposal, plus a first approximation of the suggested approach and cost for implementing the changes. Upon receipt of the Supplier's Change Estimate Proposal, NBP shall do one of the following:

a) Accept the Supplier's estimate with instructions to the Supplier to proceed with the preparation of the Change Proposal.

b) Advise the Supplier of any part of its Change Estimate Proposal that is unacceptable and request the Supplier to review its estimate.

c) Advise the Supplier that NBP does not intend to proceed with the Change.

39.2.3 Upon receipt of NBP's instruction to proceed under GCC clause 39.2.2 (a), the Supplier shall, with the proper expedition, proceed with the preparation of the Change Proposal, Following GCC clause 39.2.1. The Supplier, at its discretion, may specify a validity period for the Change Proposal, after which, if NBP and the Supplier have not reached an agreement Following GCC clause 39.2.6, then GCC clause 39.2.7 shall apply.

39.2.4 The pricing of any Change shall, as far as practicable, be calculated Following the rates and prices included in the Contract Agreement. If the nature of the Change is such that the Contract Agreement rates and prices are inequitable, the parties to the Contract Agreement shall agree on other specific rates to be used for valuing the Change.

39.2.5 The Supplier shall give an initial estimate of the cost for the Change Proposal. This initial estimate shall be at no extra cost or fee to NBP. If the initial estimate of the cost of the Change Proposal increases the Contract Price as originally set forth in the Contract Agreement by more than fifteen (15) percent, the Supplier shall notify NBP of the said increase in the Contract Price. If NBP accepts the Supplier's notification, NBP shall withdraw the proposed Change and shall notify the Supplier in writing of its acceptance. The Supplier shall not under any circumstances proceed further in the matter until it has notified NBP as aforesaid and if the Supplier does proceed with such a Change Proposal, then it shall bear its own costs if NBP rejects the Change Proposal on the grounds that it exceeds 15 percent of the Contract Price.

39.2.6 Upon receipt of the Change Proposal, NBP and the Supplier shall mutually agree upon all matters contained in the Change Proposal. NBP shall, if it intends to proceed with the Change, issue the Supplier a Change Order. If NBP is unable to reach a decision within a reasonable time, it shall notify the Supplier with details of when the Supplier can expect a decision. If NBP decides not to proceed

		with the Change for whatever reason, it shall notify the Supplier accordingly. Under such circumstances, the Supplier shall be entitled to reimbursement of all costs reasonably incurred by it in the preparation of the Change Proposal, provided that these do not exceed the amount given by the Supplier in its Change Estimate Proposal submitted Following GCC clause 39.2.2. 39.2.7 If NBP and the Supplier cannot reach an agreement on the price for the Change, an equitable adjustment to the time for achieving Operational Acceptance, or any other matters identified in the Change Proposal, the Change will not be implemented. However, this provision does not limit the rights of either party under GCC clause 6 (Settlement of Disputes). 39.2.8 Changes Originating from Supplier If the Supplier proposes a Change pursuant to GCC clause 39.1.2, the Supplier shall submit to the Project Manager, a written "Application for Change Proposal," giving reasons for the proposed Change and including the information specified in GCC clause 39.2.1. Upon receipt of the Application for Change Proposal, the parties shall follow the procedures outlined in GCC clauses 39.2.5, 39.2.6, and 39.2.7, except that the words "Change Proposal" shall be read, for the purposes of this GCC clause 39.3.1 as "Application for Change Proposal." However, should NBP choose not to proceed or NBP and the Supplier cannot come to an agreement on the change during any validity period that the Supplier may specify in its Application for Change Proposal, the Supplier shall not be entitled to recover the costs of preparing the Application for Change Proposal, unless specified otherwise in the Contract Agreement.
40	Extension of Time for Achieving Operational Acceptance	40.1 The time(s) for achieving Operational Acceptance specified in the implementation schedule shall be extended if the Supplier is delayed or impeded in the performance of any of its obligations under the Contract Agreement due to any of the following reasons: a) Any Change in the System as provided in GCC clause 39 (Change in the Solution). b) Any occurrence of Force Majeure as provided in GCC clause 38 (Force Majeure); Default of NBP; or c) Any other matter specifically mentioned in the Contract Agreement; by such period as shall be fair and reasonable in all the circumstances and shall fairly reflect the delay or impediment sustained by the Supplier. 40.2 Except where otherwise specifically provided for in the Contract Agreement, the Supplier shall submit to the Project Manager a notice of a claim for an extension of time for achieving Operational Acceptance, together with particulars of the event or circumstance justifying such extension as soon as reasonably practicable after the commencement of such event or circumstance. As soon as reasonably practicable after receipt of such notice and supporting particulars of the claim, NBP and the Supplier shall agree upon the period of such extension. In the event that the Supplier does not accept NBP's estimate of a fair and reasonable time extension, the Supplier shall be entitled to refer the matter to the provisions for the Settlement of Disputes pursuant to GCC clause 6. 40.3 The Supplier shall at all times use its reasonable efforts to minimize any delay in the performance of its obligations under the Contract Agreement.
41	Termination	41.1 Termination at NBP's convenience:

41.1.1 NBP may at any time terminate the Contract Agreement for any reason by giving the Supplier a notice of termination that refers to this GCC clause 41.1.1.

41.1.1 Upon receipt of the notice of termination under GCC clause 41.1.1, the Supplier shall either as soon as reasonably practical or upon the date specified in the notice of termination:

a) Cease all further work, except for such work as NBP may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition.

b) Terminate all subcontracts, except those to be assigned to NBP pursuant to GCC clause 41.1.2 (d) (ii) below.

c) Remove the Supplier's Equipment other than the Card hosting system/Card Management system & its allied Software and hardware from the site in its entirety, repatriate the Supplier's and its Subcontractors' personnel from the site, remove from the site any wreckage, rubbish, and debris of any kind.

d) In addition, the Supplier, subject to the payment specified in GCC clause 41.1.3, shall:

i) Deliver to NBP, the parts of the System, any material, or stationary executed by the Supplier up to the date of termination.

ii) To the extent legally possible, assign to NBP all rights, title, and benefit of the Supplier to the System, or Subsystem, as at the date of termination, and, as may be required by NBP, in any subcontracts concluded between the Supplier and its Subcontractors.

iii) Deliver to NBP all non-proprietary drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.1.3 In the event of termination of the Contract Agreement under GCC clause 41.1.1, NBP shall pay to the Supplier the Contract Price, properly attributable to the parts of the System executed by the Supplier as of the date of termination.

41.2 Termination for Supplier's Default:

41.2.1 NBP, without prejudice to any other rights or remedies it may possess, may terminate the Contract Agreement forthwith in the following circumstances by giving a notice of termination and its reasons to the Supplier, referring to this GCC clause 41.2:

a) If the Supplier becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the Supplier is a corporation, a resolution is passed or an order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if the Supplier takes or suffers any other analogous action in consequence of debt;

b) If the Supplier assigns or transfers the Contract Agreement or any right or interest therein in violation of the provision of GCC clause 42 (Assignment); or

c) if the Supplier, in the judgment of NBP, has engaged in corrupt or fraudulent practices in competing for or in executing the Contract Agreement, including but not limited to willful misrepresentation of facts concerning ownership of Intellectual Property Rights in, or proper authorization and/or licenses from the owner to offer the hardware, or materials provided under this Contract Agreement.

d) For the purposes of this clause:

i) “Corrupt practice” means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

ii) “Fraudulent practice” means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of NBP and includes collusive practices among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive NBP of the benefits of free and open competition.

41.2.2 If the Supplier:

a) has abandoned or repudiated the Contract Agreement.

b) has without valid reason failed to commence work on the System promptly.

c) persistently fails to execute the Contract Agreement in accordance with the Contract Agreement or persistently neglects to carry out its obligations under the Contract Agreements without just cause.

d) refuses or is unable to provide sufficient Materials, Services, or labor to execute and complete the System in the manner specified in the Finalized Project Plan furnished under GCC clause 19 at rates of progress that give reasonable assurance to NBP that the Supplier can attain Operational Acceptance of the System by the Time for Achieving Operational Acceptance.

e) Then NBP may, without prejudice to any other rights it may possess under the Contract Agreement, give notice to the Supplier stating the nature of the default and requiring the Supplier to remedy the same. If the Supplier fails to remedy or take steps to remedy the same within the time specified by NBP, then NBP may terminate the Contract Agreement forthwith by giving a notice of termination to the Supplier that refers to this GCC clause 41.2.

41.2.3 Upon receipt of the notice of termination under GCC clauses 41.2.1 or 41.2.2, the Supplier shall, either immediately or upon such date as is specified in the notice of termination:

a) Cease all further work, except for such work as NBP may specify in the notice of termination for the sole purpose of protecting that part of the System already executed or any work required to leave the site in a clean and safe condition.

b) Terminate all subcontracts, except those to be assigned to NBP pursuant to GCC clause 41.2.3 (d) below.

c) Deliver to NBP the parts of the System executed by the Supplier up to the date of termination.

d) To the extent legally possible, assign to NBP all rights, title, and benefit of the Supplier to the System or Subsystems as at the date of termination, and, as may be required by NBP, in any subcontracts concluded between the Supplier and its Subcontractors.

e) Deliver to NBP all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System.

41.2.4 NBP may enter upon the Project Site, expel the Supplier, and complete the System itself or by employing any third party. Upon completion of the System or at such earlier date as NBP thinks appropriate, NBP shall give notice to the Supplier that the Supplier's Equipment will be returned to the Supplier at or near the Project Site and shall return such Supplier's Equipment to the Supplier in accordance with such notice. The Supplier shall thereafter without delay and at its cost remove or arrange removal of the same from the Project Site.

41.2.5 Subject to GCC clause 41.2.6, the Supplier shall be entitled to be paid the Contract Price attributable to the portion of the System executed as at the date of termination. Any sums payable to NBP from the Supplier accruing prior to the date of termination shall be deducted from the amount to be paid to the Supplier under the Contract Agreement.

41.2.6 If NBP completes the System, the cost of completing the System by NBP shall be determined. If the sum that the Supplier is entitled to be paid, pursuant to GCC clause 41.2.5, plus the reasonable costs incurred by NBP in completing the System, exceeds the Contract Price, the Supplier shall be liable for such excess. If such excess is greater than the sum due, the Supplier, under GCC clause 41.2.5, shall pay the balance to NBP, and if such excess is less than the sum due the Supplier under GCC clause 41.2.5, NBP shall pay the balance to the Supplier. NBP and the Supplier shall agree in writing on the computation described above and the manner in which any sums shall be paid.

Termination by Supplier:

41.3.1 If NBP has failed to pay the Supplier any sum due under the Contract Agreement within the specified period, without just cause, or commits a substantial breach of the Contract Agreement, the Supplier may give a notice to NBP that requires payment of such sum with interest on this sum as stipulated in GCC clause 12.3 or specifies the breach and requires NBP to remedy the same, as the case may be. If NBP fails to pay such sum together with such interest or fails to remedy the breach or take steps to remedy the breach, then the Supplier may give notice to NBP of such events, and if NBP has failed to pay the outstanding sum, or to remedy the breach, the Supplier may give a further notice to NBP referring to this GCC clause 41.3.1, forthwith terminating the Contract Agreement.

41.3.2 The Supplier may terminate the Contract Agreement immediately by giving a notice to NBP to that effect, referring to this GCC clause 41.3.2, if NBP becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, being a corporation, if a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over any part of its undertaking or assets, or if NBP takes or suffers any other analogous action in consequence of debt. Provided, however, that a merger, amalgamation, reorganization, or reconstruction of NBP shall not give any right for termination of the Contract Agreement.

41.3.3 If the Contract is terminated under GCC clauses 41.3.1 or 41.3.2, then the Supplier shall immediately:

a) Cease all further work, except for such work as may be necessary for protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition.

b) Terminate all subcontracts, except those to be assigned to NBP pursuant to

		clause 41.3.3 (d) (ii); c) Remove all Supplier's Equipment (if any) from the site except Hardware/Software installed/deployed in NBP Premises and repatriate the Supplier's and its Subcontractor's personnel from the site. d) In addition, the Supplier, subject to the payment specified in GCC clause 41.3.4, shall: i) Deliver to NBP the parts of the System executed by the Supplier up to the date of termination. ii) To the extent legally possible, assign to NBP all rights, title, and benefit of the Supplier to the System, or Subsystems, as of the date of termination, and, as may be required by NBP, in any subcontracts concluded between the Supplier and its Subcontractors. iii) To the extent legally possible, deliver to NBP all drawings, specifications, and other documents prepared by the Supplier or its Subcontractors as of the date of termination in connection with the System. iv) To the extent legally possible, deliver/hand over to NBP all Hardware and software implemented/Deployed/installed. material in the site of NBP 41.3.4 If the Contract is terminated under GCC clauses 41.3.1 or 41.3.2, NBP shall pay to the Supplier all payments specified in GCC clause 41.1.3. 41.3.5 Termination by the Supplier pursuant to this GCC clause 41.3 is without prejudice to any other rights or remedies of the Supplier that may be exercised in lieu of or in addition to rights conferred by GCC clause 41.3. 41.4 In this GCC clause 41, the expression "portion of the System executed" shall include all work executed, Services and technical solutions provided, or other Goods acquired (or subject to a legally binding obligation to purchase) by the Supplier and used or intended to be used for the purpose of the System, up to and including the date of termination. 41.2 In this GCC clause 41, in calculating any money due from NBP to the Supplier, account shall be taken of any sum previously paid by NBP to the Supplier under the Contract Agreement, including any advance payment paid pursuant to the SCC.
42	Assignment	41.3 Neither NBP nor the Supplier shall, without the prior written consent of the other, assign to any third party (excluding the successors in interest of NBP) the Contract Agreement or any part thereof, or any right, benefit, obligation, or interest therein or there under.

6. Special Conditions of Contract (Section-VI)

The following Special Conditions of Contract (SCC) shall supplement or amend the General Conditions of Contract (GCC). Whenever there is a conflict, the provisions of the SCC shall prevail over those in the General Conditions of Contract, and in the case of a conflict between the SCC and the terms of a Contract Agreement (as defined in the SCC), the terms of the Contract Agreement shall prevail. For the purposes of clarity, any referenced GCC clause numbers are indicated in the left column of the SCC.

A. CONTRACT AND INTERPRETATION

1. Definitions (GCC Clause 1)

GCC 1.1. (e) (i)	The Country is Pakistan
GCC 1.1. (e) (iii)	The Project Site is the NBP Head Office.
GCC 1.1. (e) (x)	The Contract Agreement shall continue for consecutive (3) three years (extendable) in force until the technical solution and all the Services have been provided or unless the Contract Agreement is terminated earlier in accordance with the terms set out in the Contract Agreement.

3. Interpretation (GCC Clause 3)

GCC 3.1.1	The language of the Contract Agreement, all correspondence, and communications to be given, and all other documentation to be prepared and supplied under the Contract Agreement not otherwise specified in the Technical Requirements shall be in ***English***.

4. Notices (GCC Clause 4)

GCC 4.1	Unless specified otherwise in the Contract Agreement, notices shall be addressed to: Division Head Procurement Logistics Communications & Marketing Group National Bank of Pakistan Head Office 3rd Floor I.I. Chundrigar Road, Karachi.

5. Governing Law (GCC Clause 5)

GCC 5.1	The Contract shall be solely interpreted and governed following the substantive and procedural laws of the *Islamic Republic of Pakistan* which shall include but not be limited to the directives and circulars of the State Bank of Pakistan which may be issued from time to time.

6. Settlement of Disputes (GCC Clauses 6)

GCC 6.2.3	In the case of a dispute between the Purchaser and the Supplier, the dispute shall be referred to arbitration Following the Arbitration Act of 1940.

B. SUBJECT MATTER OF CONTRACT

7. Scope of the System (GCC Clause 7)

GCC 7.3	Delivery on time and following all terms and conditions as per Section-X – Delivery Schedule.

8. Time for Commencement and Operational Acceptance (GCC Clause 8)

GCC 8.1	The Supplier shall commence work and supply the Systems as per the Contract Agreement and Purchase Order Terms and Conditions (if any)
GCC 8.2	An operational Acceptance certificate is to be issued by NBP.

9. Supplier's Responsibilities (GCC Clause 9)

GCC 9.9	The Supplier shall have the following additional responsibilities: 1) As specified in Section VI: Technical Requirements. 2) State Bank of Pakistan and PPRA regulatory compliance for all applicable services offered by the Supplier. 3) Compliance with Secure SDLC (Security assurance activities include architecture analysis during design, code review during coding and build, and penetration testing before release.), information security standards as specified by NBP and the State Bank of Pakistan (if any). 4) The application/ system must adhere to the relevant security controls and international industry security standards/SSDLC. 5) Obtain required security clearance from the concerned authorities for their authorized staff, to keep services operational 24x7. 6) Immediate reporting of any fraudulent activity, tampering, or events noticed or observed by the Supplier at any site/locations managed or supported by the Supplier under the Contract Agreement.

10. NBP's Responsibilities (GCC Clause 10)

GCC 10.7	NBP shall have no additional responsibilities

C. PAYMENT

12. Terms of Payment (GCC Clause 12)

GCC 12.1	Subject to the provisions of GCC Clause 12 (Terms of Payment), NBP shall pay the Contract Price to the Supplier in the manner specified in the Contract Agreement.
GCC 12.3	NBP shall not pay the Supplier interest on the delayed payments.

13. Securities (GCC Clause 13)

GCC 13.2	Not applicable
GCC 13.3	The amount of performance security, as a percentage of the value of the contract not exceeding ten percent (10%) of the contract amount, which will be released after thirty (30) days of completion of the contract. The currency of the performance security shall be Pak Rupees.

14. Taxes and Duties (GCC Clause 14)

GCC 14	Bids must be inclusive of all applicable taxes, duties, levies, etc.

D. Intellectual Property

15. Copy Right

GCC 15	Intellectual Property Rights in all Custom Software and Custom Materials as specified in the Contract Agreement.

16. Software License Agreement

GCC 16	Reproduce SW for safekeeping or backup purposes Supplier hereby grants NBP license to access and use the Software, including all inventions, designs, and marks embodied in the Software

17. Confidential Information (GCC Clause 17)

GCC 17.1	There are no modifications to the confidentiality terms expressed in GCC Clause 17.1
GCC 17.6	The provisions of this GCC clause 17 shall survive the termination of the Contract Agreement for the duration provided in the Contract. Agreement.

E. Supply, Installation, Testing, Commissioning, And Acceptance of The System

18. Representatives (GCC Clause 18)

GCC 18	As per the GCC
GCC 18.2.2	As per the GCC

19. Project Plan (GCC Clause 19)

GCC 19.1	The Supplier shall undertake to supply, install, test, and commission the System Following the Finalized Project Plan as agreed to by NBP and the Contract Agreement

22. Procurement, Delivery, and Transport (GCC Clause 22)

GCC 22.5	The Supplier shall provide NBP with shipping and other documents as specified in the GCC.

23. Product Upgrades (GCC Clause 23)

GCC 23.4	The Supplier shall provide NBP with all new versions, releases, patches, and updates to all Standard, or procured Software during the Warranty/Post Warranty & Contract Agreement Periods at no cost as specified in the GCC.

24. Implementation, Installation, and Other Services (GCC Clause 24)

GCC 24	Details to be mutually agreed between NBP and Supplier at the contracting stage (Proposed conditions to be submitted as part of the proposal) applicable to GCC Clause 24.

26. Installation of the System (GCC Clause 26)

GCC 26	Installation for commissioning requires the issuance of a certificate by NBP and successful installation is not achieved unless NBP puts Systems in production.

27. Commissioning and Operational Acceptance (GCC Clause 27)

GCC 27.2.1	As per GCC
GCC 27.2.2	As per GCC

F. Guarantees and Liabilities

28. Operational Acceptance Time Guarantee (GCC Clause 28)

GCC 28.2	Liquidated damages shall be payable at a mutually agreed rate (if required)
GCC 28.3	Liquidated damages shall be assessed at the sole option of NBP at agreed milestones, such as Delivery, Installation, etc.

29. Defect Liability Guarantee (GCC Clause 29)

GCC 29.1	There shall be no exceptions or limitations to the Supplier's warranty obligations for Software.
GCC 29.4	The Warranty Period shall begin from the date of Operational Acceptance of the Systems or subsystems or as stated in RFP/Bidding documents.
GCC 29.10	During the Contract Period, the Supplier must commence the work necessary to remedy defects or damage within the timelines specified in the RFP and/or mutually agreed between NBP and Supplier from time to time, not exceeding prompt response within the timelines specified in the Contract Agreement. If not specified in the Contract Agreement, the response time shall not exceed 24 hours of notification by NBP or such other longer period as NBP may specify in writing.

G. RISK DISTRIBUTION

37. Insurance (GCC Clause 37)

GCC 37.1 (c)	Insurance will be the responsibility of the Supplier till the System is deployed.

H. CHANGE IN CONTRACT ELEMENTS

41. Termination (GCC Clause 41)

GCC 41	Either of the Parties can terminate the Contract Agreement, other than by reason of breach or non-performance or non-compliance after giving 270 calendar Days advance notice in writing (without assigning any reason).

7. Technical Specification/Requirements (Section VII)

List of Annexures

S. No	RFP Scope Details
1.	Retail/Consumer Loan Origination, Management/Monitoring System/Collection and Recovery Module (Admin module included)
2.	Corporate Loan/Monitoring System (Admin module included)
3.	Project Team Members' Resumes
4.	Client Reference Details Format
5.	Proposal Submission Format

7.1 Retail/Consumer Loan Origination, Management/Monitoring System/Collection and Recovery Module (Admin module included)

Please provide a proposal following the specifications and terms mentioned in this "Section VII".

Annexure – 1 (Requirement Specifications)

The National Bank of Pakistan (NBP) invites proposals for a robust, scalable, and secure Retail/Consumer Loan Origination System (LOS). The ideal LOS will streamline and automate various aspects of the loan origination process, from application initiation to disbursement.

Key Requirements:

- Centralized Platform: A single, integrated platform to manage all consumer loan applications.
- Real-time Processing: Efficient processing of loan applications, including approvals and disbursements (through integration).
- Comprehensive Portfolio Management: Granular insights into loan portfolios, enabling effective monitoring and risk assessment.
- Flexible Workflows: Customizable workflows to accommodate diverse loan products and processes.
- Seamless Integrations: Integration with core banking systems, credit bureaus, and other relevant systems.
- Robust Security and Compliance: Adherence to stringent security standards and regulatory requirements.
- User-Friendly Interface: Intuitive interface for both internal and external users.
- Mobile Accessibility: Mobile-friendly access for remote decision-making.

Specific Functionalities:

- Loan Origination: Application initiation, processing, and approval.
- Credit Underwriting: Risk assessment and credit decisions.
- Document Management: Secure storage and retrieval of loan documents.
- Disbursement: Efficient disbursement of loan funds.
- Portfolio Management: Monitoring, tracking, and reporting on loan portfolios.
- Regulatory Compliance: Adherence to local and international regulations.

Technical Requirements:

- Scalability: The system should be able to handle increasing volumes of loan applications and data.
- Performance: The system should provide fast response times and efficient processing.
- Security: Robust security measures to protect sensitive data.
- Integration Capabilities: Seamless integration with existing systems.

- User Experience: User-friendly interface with intuitive navigation.

Proposal Requirements:

- Detailed technical specifications
- Implementation Timeline
- Cost breakdown
- Security and compliance measures
- Support and maintenance plans

By implementing this LOS, NBP aims to enhance operational efficiency, reduce processing time, and improve customer satisfaction.

Note:

- As a part of the application scope, Legacy Data Migration is a crucial and must-have requirement.
- Escrow arrangements for source code maintenance
- System support for the required number of user logins at one point (approx.3000 concurrent logins)

Bidder Qualification Requirements for Retail/Consumer Loan Origination System

Yes – Standard Feature (fully compliant)

No – Feature not available.

The solution proposed by the Bidder should provide the below-mentioned functionalities for RLOS.

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
1.	The Bidder should be a registered entity in Pakistan in the form of Public Ltd/Private Ltd or any other form permissible under the Legal system of Pakistan and should be in business for a tenure of at least three (03) years. Relevant proof of existence (Certificate of Incorporation, Memorandum of Association, Certificate of commencement of business, Extract from the Register of Firms maintained by the Registrar etc. confirming the incorporation of the commercial entity or other relevant documents where applicable depending on the type of entity as mentioned above) shall be provided with valid tax payment documentation (FBR, Sales Tax Returns, NTN individual, NTN Company, Provincial Tax) whichever is applicable depending on type of organization (Public Ltd/Private Ltd/Partnership firm or any other form permissible under Pakistan Law). The Bidder should also be a registered taxpayer, enrolled with concerned tax authorities, and enlisted on the active taxpayer list of FBRs. The Bidder must submit copies of Tax returns /proof of payment of tax (FBR, Sales Tax Returns, NTN Company, Provincial Tax, etc.) for the last 3 years. **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence with corresponding page numbers included in the proposal.	High	For Example: Yes Reference Page Number – 98, 99
2.	Must be registered with the Sindh Revenue Board (SRB) and have active status of the registration (SNTN). **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence with corresponding page numbers included in the proposal.	High	
3.	Must have a minimum of one office/presence in any of the Karachi/Lahore/Islamabad cities of Pakistan and can provide support all over Pakistan as required.	High	
4.	Audited Profit & Loss (Income Statement) showing a turnover of Rs. 200 million aggregated during the last 3 years. The bidder should provide a letter from the company's CFO or senior management staff confirming. **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
	with corresponding page numbers included in the proposal. Vendor must submit last 03 years audited accounts with the audit firm from SBP panel of Auditors maintained under section 35 (1) of banking companies' ordinance, 1962.		
5.	Bidder should provide an undertaking on legal stamp paper 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.	High	
6.	A full-service company/agency with in-house capability of graphic design, web development, application development, creative, content, strategy, performance, lead generation, etc.	High	
7.	Bidder shall upload Declaration of Ultimate Beneficial Owners Information: • Name • Father's/Husband's Name • CNIC / Passport # • Date of Birth • Place of Birth • Address • Nationality • No. of Securities	High	
8.	Bidder must have at least three (03) expert level resources of proposed products for Proposed solution (Documentation proof List of Technical Resources / CVs must be uploaded with proper reference (page No) in the proposal)	High	
9.	Should have the in-house capability to manage end-to-end project	High	
10.	The bidder must not have existing commitments that conflict with this project's development and implementation. Bidders must disclose any current engagements with NBP related to critical systems development to identify potential conflicts. The Bank reserves the right to disqualify bidders with conflicts.	High	
11.	The bidder is required to be physically present at NBP premises to access the system through the NBP network in coordination with the assigned Project Manager and the Technical team. Remote access will not be provided under any circumstances.	High	

Functional Requirements for Retail/Consumer Loan Origination System

The solution proposed by the Bidder should provide the below-mentioned functionalities for RLOS. The list below is not exhaustive, and Bidders who offer additional functionalities over and above the list mentioned below can indicate the same in a separate list of additional features. Responses should be filled in as indicated below:

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
1.	General Requirements.		
	Maker/Checker capability at all stages.	High	
	Workflow that is customizable without the need for development	High	
	The system should have pre-defined user roles and approval limits as per criteria outlined. System to allow the administrator to change workflow/edit roles/alter authorization levels.	High	
	View Only Screen/Integration with Call Center system to show the current status of the application (day minus 1).	Low	
	Application Status was available on the NBP website through the search option.	Low	
	System to be able to extract live KIBOR rates from the Treasury system to calculate accurate markup rates and revised rates on loan anniversaries (calendar year, loan date).	Low	
	System to allow Excel-based bulk data upload for leads received through partners/off-site events, etc.	Low	
	System to have the capability to reverse/revert stage in the application process flow.	High	
	System to have the capability to upload files (jpeg, pdf, excel, word, CSV, etc.) at all stages.	High	
	System to send Email alerts to customers and Email alerts to Bank staff whenever the NBP Policy team wants. (Configurable)	Low	
	System to be able to save and print information at each stage/screen	High	
2.	Loan Application & Data Input		
	System to be able to capture Applications as per the NBP structured products. **Like:** NBP Advance Salary, Mera Pakistan Mera Ghar, Saibaan, Aitemaad Auto Hamsafar etc.	High	
	System to be able to capture Applications from Mobile Banking, Internet Banking, and Core Banking platforms in case application is input from the same.	Low	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	System to be able to capture information for Income Estimation/Assessment manually or from Core Banking through account statements by retrieving average balances and transaction tracking for salary credits, etc., after proper documentation and assessment process. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	Low	
	Detailed Data Entry of Credit Application/Proposal.	High	
	System to be able to check eligibility and alert if data entered is outside the scope defined.	Low	
	System to provide deviation options and approval mechanism based on deviation matrix.	Low	
	System to have the capability to create/generate predefined documents based on data available on LOS.	High	
	System to provide the functionality to capture the fee waiver/concession details.	High	
	System to generate automated Email Alerts (customer) and Bank staff upon the final decision of the credit application.	Low	
	System to allow for loan application review (inputter/authorizer)	High	
	System to have the capability to detect duplicate application data and also replicate application data for similar cases.	Low	
	System to be able to apply eCIB, Tasdeeq, DataCheck reader to extract data from the report and produce DBR sheet and allowable limits automatically.	High	
3.	Approval Review - Business		
	System to allow for loan application review (inputter/authorizer)	High	
	System to allow for application to be edited, marked discrepant, and returned to the origin or cancel the application. System to capture all changes to maintain an audit trail.	High	
	System to have a deduping function to trace bad matches with different criteria, e.g., phone no, address, CNIC, Company name, etc. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	System to have CAD (category-wise)/Company RACs setups.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Auto e-mail generated to an external vendor (that has a database with a huge collection of information from the nation's customers and credit reports, i.e. ICIL & BCIL) for verification, once verification is done, the same report will be uploaded to the system.	Low	
4.	Approval Review – Risk		
	System to be able to calculate Debt-Burden Ratio and other calculations based on information input (income estimation, eCIB data, etc.)	High	
	System to allow for application to be edited, marked discrepant, and returned to the origin or cancel application. System to capture all changes to maintain an audit trail. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	System to be able to assign loan limits based on data input and pre-defined parameters.	Low	
	System to provide deviation options and approval mechanism based on deviation matrix.	Low	
	System to be able to conduct Credit Scoring and loan Assessment Scoring based on pre-defined parameters and formulas.	Low	
	System to be able to capture call reports/Site Visit reports details and other reports that are required for underwriting.	Low	
	System to generate Approval, Rejection, Cancellation, & Discrepancy reports with details on a daily or need basis.	Low	
	System to generate Approval/Rejection letters as per the National Bank of Pakistan's prescribed formats.	Low	
5.	Compliance Review		
	System to be able to link with Core Banking Application to conduct OFAC, ATA, UNSC, AML/CFT checks. In case of any alert, the case is to be marked discrepant and not proceed further.	Low	
	System to share batch-wise approved list with FRMU.	Low	
6.	Post-Approval Formalities & Disbursement		
	System to generate post-approval documentation with auto-populated customer data & financing details. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	System to be able to store electronically signed contracts for post-approval documentation.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	System to allow for application to be edited, marked discrepant, and returned to the origin or cancel application. System to capture all changes to maintain an audit trail.	High	
	System to generate stage-wise TAT, Cancellation, & Discrepancy reports with details daily.	High	
	System to generate disbursement reports on a daily/need basis.	Low	
	System to capture collateral details, collateral value (market, FSV)	Low	
	System to archive documents (out of the box DMS).	High	
	The system auto-generates the Pay-order instruction and shares the pay-order details like amount, pay-order generated branch, beneficiary, etc.	Low	
	The System should calculate insurance on future depreciated values of underlying assets and divide it over installments to arrive at the total monthly payment (TMP).	Low	
	System to track deferrals, along with deferral expiry exceptions, for post & Pre-disbursement documentation. Reports are to be generated for expired deferrals.	Low	
	System to generate Letters (Offer Letters, Provisional Offer Letters, Welcome Letters, etc.)	High	
	System to generate amortization schedule and indicative term sheet as per the NBP format.	Low	
7.	Portfolio & Loan Administration		
	System to generate automated SMS/Email Alerts (customer) and email alerts to Bank staff for recoveries & collections.	Low	
	System to enable users to update recoveries and collections to ensure accurate portfolio health tracking.	Low	
	System to be integrated with Core Banking/Digital Account Opening System (CIF) to extract customer account information, bank statements, and subhead data, i.e., markup accrual and outstanding loan amounts.	Low	
	System to have options to capture the details of Balloon Payments & Early Termination	Low	
	System to track insurance and tracker on assets and initiate alerts before renewal dates	Low	
	System to have the option to revise Loan schedule post-restructuring and rescheduling.	Low	
	System to have the option for pricing structure, its revisions, and re-pricing either ad-hoc or at loan anniversary.	Low	
	System to have the option for re-booking loan post disbursal	Low	
	System to identify payment hierarchy & settlement and deduct as per hierarchy identified	Low	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	System to be able to calculate commissions/incentives based on pre-defined formulae (formulae to be editable and time-bound where applicable).	Low	
	System to be able to calculate Markup Subsidy and re-finance claims with regulatory authorities (implies two schedules to be run, one for actual markup from the client; the other for due markup from SBP)	Low	
8.	Calculations		
	Ability to automatically calculate the following:		
	• Interest Amount	High	
	• Repayment Amount (Repayment Schedule)	High	
	• Monthly Installments	High	
	• Processing Fees	High	
	• DBR & Loan Limit Calculation (%)	High	
	• Loan Maturity	High	
	• Profitability	High	
	• Grace Period Repayment schedules	High	
	• Pay Up and Pay Down repayment schedules	Low	
9.	Reports and Dashboard		
	Ability to provide reports on loan applications (hub-wise, Region-wise, Branch, Area Wise (Policy team can apply any filter to generate the report(s)). • Date wise • Branch wise • Agent wise • Source wise • Product wise • Region-wise • Loan Type • Security wise • Vendor wise	High	
	Application/Lead Status reporting	Low	
	Commission & Incentive Reports	Low	
	Markup Subsidy Claims & Other Regulatory Reports	Low	
	Portfolio Volume & ENR Reports	Low	
	Realtime TAT Reporting (Automated Email alerts and escalation built-in)	High	
	Channel/Region-Wise Sales Performance Reports	Low	
10.	Approval Matrices		
	The system should be capable enough to set up specific approval matrices from the perspective of different business domains as well as products. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	System with corresponding page numbers included in the proposal.		
	These approval matrices should be highly parameterized and simplified so that the bank's internal team should be able to make any changes in line with the approved changes in the delegation matrix in a minimum time. Such changes will come into effect at run time.	High	
	The system should have the functionality to generate the Offer Letters/Purchase orders,/Delivery Orders on a real-time basis. NBP will share the prescribed NBP format with the qualified bidder.	High	
	The system should have the functionality to generate the Sanction advice on a real-time basis. NBP will share the prescribed NBP format with the qualified bidder	High	
	The system should generate the DAC after the completion of all loan formalities (Post Approval/CAD Module). Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
11.	Workflow		
	The system should have dynamic worklist functionality that enlists all the tasks available in the worklist of the user. Flexibility should be available to configure different color schemes/themes such as based on different statuses, i.e., new task, task accepted, task viewed but not accepted, etc.	High	
	The system must generate a unique application/loan number for every application.	High	
	The system should have the ability to cancel an application, raise queries, and record replies during approval.	Low	
	The system should be able to cater to Rule-based Individual and committee-based proposal and approval routing criteria.	High	
	The system should have the ability for initiators, reviewers, recommenders, and approvers to change certain fields with proper audit trails. Existing, proposed (by each recommender), approved distinction in credit package.	High	
12.	Document Utility		

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	There should be an option available in the system to attach required documents within the credit application for ready reference of approvers/processors. These documents should be viewed with a single click without downloading to a separate folder. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should not allow alteration of any document, once the credit application is processed by the initiator and now it is available with subsequent user groups such as recommender/approver/processer. No user should be able to add/delete/update any document once the application is approved and completed unless special grants are allowed to the user ID. System to include an electronic signature option along with the end-to-end process of integration and maintenance with NBP DMS/eDMS.	Low	
	The system should have the ability to generate various letters, forms, loan legal documentation & all desired templates automatically. Provide the ability to users to update, replace, modify/configure all such letters, forms, and documents.	Low	
	The system should be able to record safe-in/Safe-out details for all documents whether "temporarily released" or "permanently released". This should be done under maker/checker authorization. For temporality-released documents, the system should generate alerts if the documents are not returned by the allowed date/time.	Low	
	Ability to track missing documents.	Low	
13.	Multi-Channel		
	The ability for customers to apply to the bank website.	Low	
	Ability to store data/documentation in the tablet in encrypted with functionality to erase automatically once transmitted to the server.	Low	
	For Customer Loan Application / Onboarding, separate Mobile app for Retail is required	Low	
	Ability to capture applications from tablets (responsive application).	High	
14.	System to prompt for Quality Assurance and Mandatory Checks upon CA submission		
	The system should generate a popup screen to prompt a "Quality Assurance Check" when the user (Relationship Manager) submits a Credit Application to relevant approval authorities. Text message upon popup screen should be user definable.	Low	
15.	User Profile Wise Dashboard of a Customer		

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	There should be a dashboard providing 360° views of a customer's relationship with the bank for all credit-related relationships.	Low	
16.	Email Alerts/Notifications		
	The system should generate email alerts when a task is generated for a user/user group, and when an action is taken on a credit application. The system should keep on generating alerts based on user-definable frequency until the required action is performed by the target user. Automatically generate email notifications for escalation if an application/ task exceeds defined processing time thresholds.	High	
	Email alert contents and audiences should be user-defined.	Low	
17.	Audit Trail/Audit Logs		
	Audit Trails/logs should be available for all data input screens and approval processes. Audit logs should contain a field, screen/form level logs as well field level logs, and changelogs for document management utility. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Auto Sync of App & DB between PR and DR, with comprehensive DR switchover manuals.	High	
	Audit Trails/logs should be available for all processes, transactions, and Static Data updates (including user/role maintenance).	Low	
	Audit logs should contain screen/form level logs as well field level logs.	Low	
18.	Decision-Making through Smartphone		
	The system should be compatible and responsive enough to give a user-friendly interface on any Smart Mobile/Table-based browsers.	Low	
19.	LogBook/Task Tracking Sheet		
	The system should have a feature to display the TTD/In Hands task MIS to the user and its Reporting to users along with task details.	High	
20.	Help & FAQs		
	The system should have the feature that when the mouse hovers over any Tab/Accordion, it will be described as that item.	Low	
	In the configuration setup, the system will provide an option to update the description of that field. So, when the mouse hovers on any tab/Accordion it will provide the description.	Low	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	The system should have built-in FAQ features for user support	Low	
21.	Geographical Tagging & Tracking		
	The Smart Applications will be fully supported with geo-tagging & Tracking to create a complete travel journey or to record the geotagging of client location for further monitoring and should be able to get coordinates from GPS even in the offline mode.	Low	

Technical Requirements

The solution proposed by the Bidder should provide the below-mentioned technical requirements for RLOS. The list below is not exhaustive, and Bidders who offer additional technical requirements over and above the list mentioned below can indicate the same in a separate list of additional features. Responses should be filled in as indicated below.

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
1.	Service Oriented Architecture (RESTful, SOAP Microservices)	High	
2.	Web-based solution.	High	
3.	The system should have a standard menu structure	High	
4.	User-friendly Graphical User Interface	High	
5.	Data Purging, Archiving & Data Warehouse Support	High	
6.	Supported file formats	High	
7.	Data Encryption & Security Support	High	
8.	Multi-Language	Low	
9.	Multi-entity, multi-currency	High	
10.	Parameterization and Customization (Entire Application)	High	
11.	Business Process Management Capability/Integration	High	
12.	Compliance with Regulatory Requirements	High	
13.	Software Development Platform/IDE	High	
14.	Network related Requirements	High	
15.	Segregation of Functional and Security/ Admin modules	High	
16.	Big Data Integration	Low	
17.	Business Intelligence Capability	Low	
18.	Business Continuity and DR availability	High	
19.	Change, Patch & Release Management Process	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
20.	Data Migration Techniques & Methodology	Low	
21.	Compliance with Regulatory Requirements	Low	
22.	Version Upgrades	Low	
23.	Single Sign-On (SSO) Support & Integration with Enterprise Identity and Access Management Solution	Low	
24.	Log Files & Audit Trail	High	
25.	Data Integration	High	
26.	Is it possible for a user to choose his or her role from a standard list of organizational roles specifically for the Loan Origination Module?	Low	
27.	The platform must support integration with XML, JAVA, MySQL, PostgreSQL, Oracle Database, Microsoft SQL Server, and Visual Studio via ISO-based standards.	High	

Identity and Access Management (for User/Role Management)

The system should have prudent Identity & Access Management functionality. This functionality should contain:

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	Maker & Checker functionality All user and role management functionality should be performed under the four-eye principle, wherein the maker will execute/initiate any request, and the checker will approve the same.	High	
2.	Privileges for Identity & Access Management Team Responsibilities should be segregated by defining specific roles for teams with different responsibilities and roles. For all user and role maintenance-related tasks, a separate role should be available so that the team having such a role should be able to perform end-to-end tasks about user/role maintenance only. Besides, they should not be able to perform any business/transaction activity other than user/role maintenance.	High	
3.	User/role maintenance-related logs and reports Comprehensive reports/logs should be available for periodical reviews. Logs and reports should be available to monitor:	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
	o User-based reports enlist what roles are assigned to each user. o Roles-based reports enlist all users with the specific assigned role. o Report listing all privileges assigned to the specific role. o A report should be available to review all roles, along with the aggregate list of privileges assigned to each user. Privilege type should be specifically mentioned against each form, e.g., Create, Update, Delete, View, etc. o A user maintenance review report will be required. o Field-level logs will be required for monitoring every amendment in user/role maintenance. o ID Management team's activity logs and reports		
4.	Reports for users created/modified/disabled period-wise filters	High	
5.	History maintained role modifications.	High	

Checklist for User ID & Role Management

Responses should be filled in as indicated below:

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	Are ADMIN IDs escrowed?	High	
2.	Is the user ID disabled by the application after the non-usage of the user ID as per the NBP AD Policy?	High	
3.	Is user password change enforced as per NBP AD Policy	High	
4.	Is the user ID disabled by the application after three invalid login attempts as per NBP AD Policy?	High	
5.	One-Time Password: Does the application prompt for a change of password after 1st login?	High	
6.	Is user password complexity enforced/applied as per NBP Policy?	High	

S. No	Functional Requirements	Priority	Response (Yes / No)
7.	Is a maker/checker available for user ID creation and amendments?	High	
8.	Is a separate role for user access management available & restricted to access management only?	High	
9.	Are audit logs and user modification logs available?	High	
10.	Is the Access Rights Matrix available?	High	
11.	Is integration with Single Sign-On (SSO) available?	Low	
12.	Can an Identity & Access Management (IAM) user (with Role Change rights) assign roles to himself?	Low	
13.	Is the user ID disable option available on the user ID amendment screen?	Low	
14.	Is a password reset option available in the end-user application?	Low	
15.	Is the Remarks/Description field available on user ID creation and amendment screens for user request reference?	Low	
16.	Is a user guide available for user access management (please share)?	Low	
17.	Admin or any privileged generic ID should not be used for any BAU activities.	High	

General Requirements

Responses should be filled in as indicated below:

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	The system should be compliant with the State Bank of Pakistan's regulatory policies.	High	

S. No	Functional Requirements	Priority	Response (Yes / No)
2.	The system should be compliant with standard Information Security Requirements as specified by the Bank's IS function from time to time.	High	
3.	The system should offer the "Forgot Password" option so that the user can generate a new password without reference to the "Identity & Access Management" team.	High	
4.	The System is to have integration support available to fetch customer information (CIF details) from the Core Bank System. The system will always pull such data from the Core Banking System and will never push client information to the Core Banking Application.	High	
5.	Parameterization: The system should be highly parameterized to add any change in: a. Approval matrix/business process flow at the run with ensuring uninterrupted flow/execution. b. Approval Matrix update/Create business rules and matrices with breakthrough ease. c. Approval authorities update recommenders and approvers. d. Parameterized Product Structure Management/Product Management/Security Management. e. Business Hierarchy/Role Hierarchy Management f. Static Data update for all functionalities g. Filed addition in forms/screens on a need basis. h. Branches NBP Region, Clusters, Areas or Branch	High	
6.	System to allow all such changes to be incorporated by the bank's user from UI without vendor engagement.	High	
7.	System to control data access using roles and authorization overrides.	High	
8.	The system should be able to migrate data from legacy applications to another new platform.	High	
9.	Escrow arrangements for source code maintenance	High	

S. No	Functional Requirements	Priority	Response (Yes / No)
10.	Knowledge transfer to NBP's team for incorporating necessary changes in the system to cater to future requirements.	High	
11.	Experience of the Bidder: The Bidder must demonstrate a proven track record of successful Retail Loan Origination System (LOS) deployments and implementations. Specific Requirements: Minimum of one (1) successful Retail LOS implementation in Pakistan (Commercial Bank). Comprehensive Documentation: Provide evidence such as signed purchase orders, work orders, agreements, and client references to substantiate the claimed experience. Unverified Documentation: Unsigned and unstamped documents will not be considered. Evaluation Criteria: All credentials and other evaluation criteria will be assessed as of the RFP closing date, excluding financial information.	High	
12.	TAT Monitoring (User wise, Profile wise & Segment wise)	High	
13.	SMS & Email Alerts and Notifications	High	
14.	SLAs & Escalations	High	
15.	RM/ARM Shuffle	Low	
16.	Authority Swap (Vertical & Horizontal)	Low	
17.	Customized Reporting and Dashboards	High	
18.	Error Handling (Generic Functionality)	Low	
19.	Group Chat	Low	

S. No	Requirements	Response
1.	Describe in detail the scalability features of the platform.	

S. No	Requirements	Response
2.	Details of the Security Model Used by the Platform for Protecting the NBP and its Customers.	
3.	How does your Platform manage user profiles and group management?	
4.	What is the Language platform used to develop the solution? e.g., JAVA, .net, node JS, python, etc.	
5.	What is the development methodology?	
6.	What are the supported Application Server Platforms?	
7.	What are the front-end Frameworks?	
8.	What is the minimum hardware requirement? Keeping in view the number of Retail Users (3,000), Retail Credit Proposal Volume (+ 300,000)? Note: Attach the separate annexure with detailed Hardware Requirements in the Bill of Quantity (Section X). Recommend the detailed infrastructure with specifications required for rolling out the solution, including (but not limited to) hardware, Operating System, database, middleware, replication technologies/tools, version management tools, software licenses, and support subscription.	
9.	What is the LOS Platform Architecture and Components Diagram (with/without high availability) and disaster recovery (DR) sites	
10.	What are the other pre-built integration components supplied with the platform?	
11.	Provide details on the platform's integration with the bank's legacy system or third-party fintech and aggregators.	

Information Security-Related Requirements

Application Security Review Checklist

Application Security Review Checklist

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
1.0	**Application Components**	Acceptable Criteria	
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 usernames.	
2.6	**Initial Password** Does the application prompt to change the initial password?	Default passwords are changed following installation of system or software. Initial password should be pre-expired. Application should immediately prompt to change the initial password upon users first log into the application. Applications are configured to enforce password change upon first login whenever temporary password is issued (e.g., account re-activation after account lock out, or password reset request, etc.). In all cases, user authentication should be ensured, either by asking old password or by sending reset link to registered email address, etc.	
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 disabled autocomplete	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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: i. Password history should be maintained for at least 6 passwords. ii. Password Should be hard to guess. It should not constitute with the common predicted phrases like names, Tel Number, Date of Birth, Anniversary, same as username etc. iii. Password must be Alpha-Numeric with both upper and lower case characters (e.g., a-z, A-Z) iv. Password change interval must not be less than one (1) day. v. Must have at-least one numeric and one special character e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) vi. Account should be locked after 5 unsuccessful login attempts, and should only be unlocked upon receipt of request from valid user to the administrator or 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. **Privilege Level** • Minimum 12 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 username 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 username Password should not be easily guessable passwords e.g. 12345678, asdfasdf, etc. Password should not be blank. Static passwords must never be displayed on the screen in clear text.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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. Application forcefully terminates all existing session when the user logs out and/or web browser is closed without logout. After successful logout from the application: All Session parameters on client side and server side should be removed. Application should not resume the session upon manual redirection to previous page. Application should not allow the cached version of authenticated pages.	
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 show by the application	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
3.3	**Entitlement Review report** Does the application provides the complete details of all user's 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. User and Access Management should be independent, not managed by the same team who is performing business operations/tasks in the application.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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**		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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 usernames 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 including data in logs and data in backups (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. Special characters should not be allowed as input. If needed, whitelist the characters which can be accepted.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 in place 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**		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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/requirement, 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)	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
		• 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 preventing 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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**		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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, Default application/DB/OS accounts should be identified and disabled where possible. If cannot disabled, default password should be changed with whitelisting and also define the ownership of these accounts. Service/functional accounts should be identified and their purpose shall be documented and approved by the relevant senior management along with the defined ownership and protection of credentials in storage and transmission. Service accounts should not have interactive login rights unless there is a valid business or technical need. Passwords for service/admin accounts should be in dual controlled as split knowledge and escrowed or managed via privileged id management solution.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
		Password of these accounts should be more complex.	
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. Access to audit logs including administrative activities is restricted for access. Audit logs should be protected against data tempering and un-authorized access. Credentials, PAN, PII, PIN block, etc. must not be the part of logs in plain text.	
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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. Default application/DB/OS accounts should be identified and disabled where possible. If cannot disabled, default password should be changed with whitelisting and also define the ownership of these accounts. Service/functional accounts should be identified, and their purpose shall be documented and approved by the relevant senior management along with the defined ownership and protection of credentials in storage and transmission. Passwords for service/admin accounts should be in dual controlled as split knowledge and escrowed or managed via privileged id management solution. Password of these accounts should be more complex.	
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. Service accounts should not have interactive login rights.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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 Idle session timeout in applications is set to 5 to 15 minutes, based on asset classification.	
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. Authentication session ID should be changed upon each login.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 to 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 in config file. It should not be hardcoded. 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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 Information 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 been 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 Application Security

Web Secure Coding Checklist		
The ITPM should complete this checklist with the project's developers in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.		**Answer (True, False, N/A)**
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. user authentication should be ensured, either by asking old password or by sending reset link to registered email address, etc.	
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 Or when password is changed.	
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 upon each login.	
3.8	The session id is changed upon 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 "HTTP Only".	

3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and 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. Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.	
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) 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 account Balance, 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) 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 escaped properly.	
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or escaped properly.	
6.6	All untrusted data that are output to any interpreters not specifically listed above 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. Encrypt all data in transit with secure protocols such as TLS with forward secrecy (FS) ciphers,	
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 invalidated 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 HTTP Only 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

API Security Review Checklist

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
1.0	**Authentication & Authorization**	Acceptable Criteria	
1.1	Use secure authentication mechanism	Do not 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 Authority 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 instead of HTTP	Implement SSL based communication over API connections.	
2.2	Display as minimum information as possible in you API request/response	Do not 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	Do not use any sensitive data (credentials, passwords, security tokens, and/or API keys) in the URL but use standard Authorization header.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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-URL encoded, 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 decency 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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: Same origin (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	• Eternal entities' 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**		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		**Guide**	**Answer (True, False, N/A)**
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.	

Database Security

Database Security Controls Requirements

Vendor to share technical documents/evidence/responses for the following database security controls requirements:

1 The database solution offered by the vendor must support password configuration / control parameters for database privilege / named users which at a minimum includes:

Minimum Length

- The password must be of minimum eight characters in length for standard user IDs and twelve characters for administrative/privilege IDs.

Complexity:

- Must be Alpha-Numeric with both upper and lower case characters (e.g., a-z, A-Z)
- Must have at-least one numeric and one special character e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

History.

Same password was not used within at-least the last 6 changes.

Account Lockout

Password must be locked out after 5 failed login attempts.

Password Expiry

Passwords are forced to be changed after 1 month.

The database must have capability to change passwords of default and unused database accounts.

2 The database solution 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.

3 The database must provide best-practice security configuration as per industry leading compliance standards, such as CIS benchmarks.

4 The database platform must provide native capability of data encryption to protect customer PII / confidential data stored in back office database tables. Database encryption should be flexible to implement on complete

Vendor to share technical documents/evidence/responses for the following database security controls requirements:	
	database, table space or at column level. In addition, Database should be flexible to support integration with any 3rd party database encryption solutions. Vendor also required to share technical documents / evidence pertaining DB encryption standard and process for secure management of DB encryption keys.
5	The database should provide native capability of data redaction/masking to protect customer PII data / confidential data on test database environment. In addition, Database should be flexible to support integration with any 3rd party data masking/redaction solutions.
6	The database should provide role-based-access control at the granular level and allow database administrator to centrally manage roles and privileges of database users.

Infrastructure Security

- The solution must be compatible with OS CIS controls (Linux/Microsoft).

7.2 Corporate Loan/Monitoring System (Admin module included)

Please provide a proposal following the specifications and terms mentioned in this "Section VII."

<u>Annexure – 2 (Requirement Specifications)</u>

NBP seeks a robust Loan Origination System (LOS) to streamline and automate credit processes across various business segments, including:

• CIBG	-	Corporate & Investment Banking Group
• MM (IDG)	-	Middle Market (Inclusive Development Group)
• SE	-	Small Enterprises
• IDG	-	Inclusive Development Group
• Agriculture	-	Rural Bank
• IFRG	-	International, Financial Institutions & Remittances Group
• SAMG	-	Special Asset Management Group
• NBP Aitemaad Islamic	-	Islamic Banking
• R & CP	-	Risk & Credit Policy
• CAD	-	Credit Administration Department

Key Functional Requirements:

- Loan Origination: Automated processing of credit applications, from initiation to pre-disbursement.
- Credit Monitoring: Real-time tracking and analysis of credit portfolios.
- Reporting and Analytics: Comprehensive reporting and data analytics capabilities.
- Integration: Seamless integration with core banking systems and other applications.

Key Features:

- Real-time Decision Making: Enable rapid credit decisions from any location.
- Flexible Workflows: Customizable workflows to accommodate various credit products and processes.
- Automated Processes: Streamline operations with automated tasks and document generation.
- Robust Security: Protect sensitive data with advanced security measures.
- Scalability: Adapt to future growth and evolving business needs
- Mobile Accessibility: Mobile-friendly access for remote decision-making.

Bidder Qualification Requirements for Corporate Loan Origination System

Yes – Standard Feature (fully compliant)

No – Feature not available.

The solution proposed by the Bidder should provide the below-mentioned functionalities for CLOS.

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
1.	The Bidder should be a registered entity in Pakistan in the form of Public Ltd/Private Ltd or any other form permissible under the Legal system of Pakistan and should be in business for a tenure of at least three (03) years. Relevant proof of existence (Certificate of Incorporation, Memorandum of Association, Certificate of commencement of business, Extract from the Register of Firms maintained by the Registrar etc. confirming the incorporation of the commercial entity or other relevant documents where applicable depending on the type of entity as mentioned above) shall be provided with valid tax payment documentation (FBR, Sales Tax Returns, NTN individual, NTN Company, Provincial Tax) whichever is applicable depending on type of organization (Public Ltd/Private Ltd/Partnership firm or any other form permissible under Pakistan Law). The Bidder should also be a registered taxpayer, enrolled with concerned tax authorities, and enlisted on the active taxpayer list of FBRs. The Bidder must submit copies of Tax returns /proof of payment of tax (FBR, Sales Tax Returns, NTN Company, Provincial Tax, etc.) for the last 3 years. **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence with corresponding page numbers included in the proposal.	High	For Example: Yes Reference Page Number – 200, 201
2.	Must be registered with the Sindh Revenue Board (SRB) and have active status of the registration (SNTN). **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence with corresponding page numbers included in the proposal.	High	
3.	Must have a minimum of one office/presence in any of the Karachi/Lahore/Islamabad cities of Pakistan and can provide support all over Pakistan as required.	High	
4.	Audited Profit & Loss (Income Statement) showing a turnover of Rs. 200 million aggregated during the last 3 years. The bidder should provide a letter from the company's CFO or senior management staff confirming. **Note:** To demonstrate compliance with the specified requirement, please attach the documentary evidence	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
	with corresponding page numbers included in the proposal. Vendor must submit last 03 years audited accounts with the audit firm from SBP panel of Auditors maintained under section 35 (1) of banking companies' ordinance, 1962.		
5.	Bidder should provide an undertaking on legal stamp paper 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.	High	
6.	A full-service company/agency with in-house capability of graphic design, web development, application development, creative, content, strategy, performance, lead generation, etc.	High	
7.	Bidder shall upload Declaration of Ultimate Beneficial Owners Information: • Name • Father's/Husband's Name • CNIC / Passport # • Date of Birth • Place of Birth • Address • Nationality • No. of Securities	High	
8.	Bidder must have at least three (03) expert level resources of proposed products for Proposed solution (Documentation proof List of Technical Resources / CVs must be uploaded with proper reference (page No) in the proposal)	High	
9.	Should have the in-house capability to manage end-to-end project	High	
10.	The bidder must not have existing commitments that conflict with this project's development and implementation. Bidders must disclose any current engagements with NBP related to critical systems development to identify potential conflicts. The Bank reserves the right to disqualify bidders with conflicts.	High	
11.	The bidder is required to be physically present at NBP premises to access the system through the NBP network in coordination with the assigned Project Manager and the Technical team. Remote access will not be provided under any circumstances.	High	

Functional Requirements for Corporate Loan Origination System

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
1.	Credit Application Initiation, Approval & DAC Issuance		
	The system should be capable enough to handle credit application initiation/approval for multiple categories of business (legal entities), e.g., Group-based entities, partnerships, FI, DFIs, Exchange Companies, as well as individuals.	High	
	The system should also be capable of handling Disbursement Authorization (chronological assignment) and integration with allied core banking solutions operating in the NBP.	Low	
	System to be able to capture Applications as per the NBP structured products. System to be able to capture Applications from Mobile Banking, Internet Banking, and Core Banking platforms in case application is input from the same.	Low	
	System to have the capability to detect duplicate application data and also replicate application data for similar cases. The system to have a deduping function to trace bad matches with different criteria, e.g., phone no, Legal ID, address, CNIC, Company name, etc. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	System to be able to apply eCIB/Tasdeeq reader to extract data from the report.	Low	
2.	Obligor Management		
	The system should be able to capture demographic and other key data elements, Management, Ownership & Shareholder, Country Rank/World Rank (for FI customers), and other borrowing information reports (BIR). Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
3.	Regulatory Sector and Industry		
	The system should be able to display the list of all regulatory sectors and industries configured at the Credit Policy level, along with assigned regulatory codes.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.		
4.	Credit Application Initiation (Economic Group & Individual)		
	The system should handle initiating Credit Applications for all existing clients (having a valid unique client ID) and new clients who do not have any existing relationship with NBP; hence, there is no unique client ID available, along with the end-to-end process of integration and maintenance.	High	
	The system should allow automatic fetching and population of information in relevant screen fields for an existing customer (data reusability), for example, Customer Profile, Exposure Details, Economic Group Exposure, Existing Facility Details, Limit details, Classification details, Collateral/Security details, Equity Investment, etc.	Low	
	The system should be designed to possess the capability of seamless integration with the Pakistan Stock Exchange (PSX), aiming to acquire essential information about obligors. This integration streamlines the credit evaluation process, empowers lenders with accurate and timely information, and ultimately contributes to more informed and prudent lending decisions.	Low	
5.	Facility and Security structure		
	The system should serve the requirement of the main limit and ‘n’ number of sub-limit functionality (Parent, Child, and Sub Child) along with economic group interchangeable limits and sub-allocation of limits. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The user should be able to select desired facilities from a pre-defined/customizable list of the bank’s products/facilities and capture all relevant information regarding the limit amount, expiry date, pricing, security/collateral, the number of drawdowns, etc. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should be able to capture detailed security/collateral information against respective facilities. Wherein multiple securities/collaterals (e.g., one to one, one to many, many to one, many to many) can be assigned to a single facility, or a single security/collateral can be assigned to multiple facilities, having the same or different currencies.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.		
	The system should be able to calculate and perform the Collateral Cushion Analysis.	Low	
	The system should have the capability to handle the Initiation & Approval of Multiple EOLs (in a single day or on different dates) against the Same customer/limit and thereafter Track Maturities/Expiries of the respective approved EOLs. The system should provide details of the number of approvals during a certain period for each customer.	Low	
	The system should have the option to set up and configure facilities/limits through administration setup. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should have the ability to earmark limits at the main as well as sub-limit levels within economic group entities at the group and entity levels as well.	Low	
	The system should have the ability to capture details of Subordinated Loans.	Low	
	In the event any collateral is to be released, the system should have the capability to check whether the remaining collateral adequately covers the exposure and trigger the same to the relevant authorities.	Low	
	The system should have the ability to capture Account Behavior in Working Capital Finance.	Low	
	The system should have the ability to capture Liquid collateral details - Eligible as per IFRS-9 standards.	Low	
	The system should be able to feed Country & Financial Institution limits (for FI credit proposals)	High	
	The system should be able to record one-off limits, feeding on tranche-based/partial limits.	High	
	The system should be able to feed the Name of External Collateral Rating Agency, External Collateral Rating - Short Term, and External Collateral Rating - Long Term. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
6.	Other Calculators		

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	The system should have the feasibility to customize different credit evaluation calculators/calculations with less effort/low code as per The National Bank of Pakistan format: • Capital Charge Calculation • CAPEX Details Exhibit • Working Capital Calculation • Group Exposure Calculation • Earning and Deposit Exhibit • etc.	Low	
7.	Financial Analysis		
	The system should have functionality for comprehensive financial analysis of customers. Financial Analysis should encompass, but is not limited to, Balance Sheet, Profit & Loss account, Ratio Analysis (Liquidity Ratios, Leverage Ratios, Profitability Ratios, etc.), Cash Flow (Manual and Automated) Analysis, Industry/Sub-industry Peer Analysis, Financial projections for long-term loans, Compliance with regulatory requirement/minimum threshold; etc.	High	
	Such functionality should be able to utilize historical and current data as required by the bank.	High	
	There should be separate key modules for each industry considering comprehensive parameters. It should have the flexibility to add/remove/edit parameters to analyze current and projected financials.	Low	
	The system should maintain and generate MIS of Financial and Non-Financial historical data of the borrower. This will be required for the development of statistically driven ORR models.	Low	
	Admin module to configure or update any Chart of Accounts (business segment-wise) throughout the application journey. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Financial data for the customer can be uploaded using Excel-based files on the defined structures.	Low	
	Data should allow users to feed "Audited/Unaudited" as well as "Annual/Quarterly/Semi-Annual" financials, etc. periods. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
8.	Risk Rating and PD Calculation		
	Industry-wise Calibration: Ability to customize risk ratings based on specific industry factors.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.		
	Obligor-level Rating: Assign risk ratings to individual borrowers (ORR model) Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Facility-level Rating: Assign risk ratings to individual credit facilities (FRR model). Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Segment-specific ORR Modules: Separate ORR modules for different segments (Corporate & Commercial, SE & ME, Agriculture, Individual, Financial Institutions, Micro Finance Banks, etc.).	High	
	Configurable Business Rules: ORR and FRR models adhere to configurable business rules aligned with credit policies and procedures.	High	
	The system should be capable of generating the Economic Group Risk Rating (obligor & facility) and maintaining the historical data for Risk Ratings and overrides.	Low	
	The system should be capable of capturing the Quantitative and Qualitative or financial and non-financial Risk Factors. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should have the configurable industry-accepted 'Risk Appetite Framework.'	Low	
	The system should be capable of generating MIS of historical data for Risk Ratings and overrides.	High	
	The system should be capable of generating the Environmental and Social Risk Ratings (ESRM) of retail, trade, microfinance, small and medium enterprises (SMEs), corporate finance, and project finance under the SBP Green Banking Guidelines (GBGs) for Pakistan's financial sector and built-in Monitoring Checklist.	Low	
	Configurable Business Rules: ORR and FRR models adhere to configurable business rules aligned with credit policies and procedures.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Audit Trail: The system logs all manual overrides, including date, timestamp, workstation ID, user ID, and before/after values.	Low	
9.	Capital Adequacy Ratio Calculation (RWA)		
	The system should have inbuilt functionality to calculate the Minimum Capital Requirement (as per the SBP Guidelines) based on Risk-Weighted Assets by calculating the Cash Conversion Factor (CCF), EAD, Basel Eligible Collateral Value in each FL, and NFL facility level.	Low	
10.	International Financial Reporting Standard (IFRS) – 9		
	The system should have inbuilt functionality to calculate the IRR, EDA/NPV, PD, LGD, CCF, and CEL for IFRS 9 reporting purposes.	Low	
11.	Large Exposure Calculation		
	The system should have inbuilt functionality to mark the customer as a Large Exposure at the credit application level on a real-time basis.	Low	
12.	Limit Allocation Module & Lending to for FI Business Details		
	The system should have inbuilt functionality to record and streamline the Limit Allocation and Lending to FI Business (Domestic and International) to monitor the FI exposure as per the Regulatory requirement.	Low	
	This functionality should be designed to comply with the Regulatory requirements and enable the monitoring of FI exposure with accuracy and reliability.	Low	
13.	Exception, Condition, Consideration & Covenant Management		
	The system should have inbuilt functionality to display the preconfigured Exceptions. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	<u>Business User Screen:</u>		
	The system will provide the ability to select the Exceptions from the list with Yes, No, and NA options, based upon the 'Yes' selection, the user will be able to add the information in the text box provided on that specific Exceptions record. A small pop-up (Heading _ Business Justification) will be required to capture the comments. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	<u>Risk User Screen:</u>		

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	The system will provide the ability to approve, reject, or defer (by selecting or clicking the checkbox) the exception against each non-Compliant exception, upon selecting any action, the system will ask in the same pop-up (Heading _ Risk Remarks) to update the remarks just after the business user justifications. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	In case of the selection of the Defer option, the system will display the Calendar and allow Risk users to select the future date (selection of current date or past date is not allowed). After that, the system will generate a notification (20 days before the set date) to the RM and other business and risk users stating that the due date has arrived please take corrective action.	High	
14.	Call Report		
	Separate routing of Call Reports to the required level for review as per frequency defined in the policy as well as more frequently on a need basis. Routing of call reports should be allowed other than BCAs so all stakeholders remain abreast of recent developments. Call reports will not have any workflow; it is a separate and stand-alone activity.	Low	
15.	Checklist Execution		
	The system should have the functionality to execute a checklist before a credit application is submitted to relevant approval authorities. The checklist will contain a user-defined name along with a document attachment option against each checklist item. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
16.	Approval Matrices		
	The system should be capable enough to set up specific approval matrices from the perspective of different business domains as well as products.	High	
	The system should also allow the set-up of the Shariah compliance/Shariah Board roles in Islamic financing approvals.	High	
	These approval matrices should be highly parameterized and simplified so that the bank's internal team should be able to make any changes in line with the approved changes in the delegation matrix in a minimum time. Such changes will come into effect at run time.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	The system should also allow addition/deletion/update of any tier therein. System to ensure uninterrupted execution of all in-process credit applications where any change has been incorporated in the existing approval matrix. The system should have the capability to enable the user to select approval tier selection in case of a change in approval structure or absence of any authority and forward credit application to the next tier.	High	
	Such approval matrices should follow business/branch hierarchy, defined/ sourced as static parameters so that credit application is routed to the desired user group(s).	Low	
	The system should also have the functionality to generate a task in the worklist of a user group. This will be helpful in the execution of a task by an acting authority in the absence of the respective user.	Low	
17.	Workflow		
	The system should have dynamic worklist functionality that enlists all the tasks available in the worklist of the user. Flexibility should be available to configure different color schemes/themes based on different statuses, i.e., new tasks, Task accepted, task viewed but not accepted, etc.	High	
	The system must generate a unique application/loan number for every application.	High	
	The system should have the ability to cancel an application, raise queries, and record replies during approval.	Low	
	The system should be able to cater to Rule-based Individual and Committee proposal and approval routing criteria Approval through Circulation or Conduct a Meeting' (Simultaneous approval options should be enabled for Credit Committee members).	Low	
	The system should have the ability for initiators, reviewers, recommenders, and approvers to change certain fields with proper audit trails. Existing, proposed (by each recommender), approved distinction in credit package. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
18.	Document Utility		
	There should be an option available in the system to attach required documents within the credit application for ready reference of approvers/processors. These documents should be viewed with a single click with or without downloading them to a separate folder.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.		
	The system should not allow alteration of any document once the credit application is processed by the initiator, and now it is available with subsequent user groups such as recommender/approver/processer. No user should be able to add/delete/update any document once the application is approved and completed unless special grants are allowed to the user ID. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should have the ability to generate various letters, forms, loan legal documentation & all desired templates automatically. Provide the ability to users to update, replace, modify/configure all such letters, forms, and documents.	Low	
	The system should allow amendments in standard templates for further utilization.	Low	
	The system should be able to generate a list of pending cases in the queue. The user can also view the total Disbursement Authorization Certificate (DAC) pending within their jurisdiction.	Low	
	The system should be able to generate an indicative term sheet.	Low	
	The system should maintain a repository of all previous approvals along with associated documents attached to the proposal for audit purposes and easy retrievals as and when needed. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Post approval, the system should enable the selection of BLA from the system for genuineness confirmation and security perfection.	Low	
	The system should be able to capture the details of syndicate financing separately details, including the share of other banks where NBP is a leading or participating Bank.	Low	
	The system should be able to maintain standard templates of Legal documents, including financing, security, and control documents. Once the facility is approved, the documents can be selected, filled, and printed from LOS.	Low	
	The system should prepare the Documentation Checklist (DCL) based on the business segment.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.		
	The system should prepare the Documentation Check List (DCL) based on the Facility selected. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should prepare the Documentation Check List (DCL) based on the Collateral/Security. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should have the functionality for the tracking movement of documents, including system-based safe-ins and Safe-outs.	Low	
	The system should be able to maintain the relevant digital registers at centralized/regionalized CAD locations, such as miscellaneous security registers, DAC Issuance registers, etc., within the LOS.	Low	
	The system should be able to record deficiency/deferral in documents and generate triggers on assigned due dates.	Low	
	The system should also have the feature of recording the relevant details of deferrals allowed, date of deferral allowed/due dates, type of deferral (critical, semi-critical, etc.), authority for allowing deferral, and any extension in already allowed deferral. The document subsequently received shall also be updated accordingly.	Low	
	The system should be able to manage the Documentation (Documentation Management System) based on workflow/process flow at pre and post approvals. **Note:** To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	The system should be able to simultaneously manage credit vendors' nominations/selection and allocation based on workflow/process flow at pre and post-approvals.	Low	
19.	Task Reassignment		

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	The system should allow re-assigning an accepted/in-process credit application to a different user in case of unavailability of a user or wrong assignment. There should be an option to enable maker & checker functionality for this reassignment functionality. Such re-assignment is to be done under proper authentication by a selected user group only.	Low	
20.	System to prompt for Quality Assurance and Mandatory Checks upon CA submission at every stage.	Low	
	The system should generate a popup screen to prompt a "Quality Assurance Check" when the user (Relationship Manager) submits a Credit Application to relevant approval authorities. Text message upon popup screen should be definable.	Low	
21.	Data Reusability		
	The system should be able to extract/populate information from previous credit applications of the same borrower/group. Users should be able to change the required information in the new application, whereas data from previous credit applications will remain unchanged. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
22.	User Profile Wise Dashboard of a Customer		
	There should be a dashboard providing 360o views of a customer's relationship with the bank for all credit-related relationships.	Low	
23.	Reporting and Analytics		
	The system should be capable enough to: Access real-time reports, including TAT and logbook reports, quickly and easily using dashboard or reporting functionality. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Built-in Regulatory Reports (frequency: weekly, monthly, Semi-annually, Annually, and on-demand)	High	
24.	Email Alerts/Notifications		
	The system should generate email alerts when a task is generated for a user/user group and when an action is taken on a credit application. The system should keep on generating alerts based on user-definable frequency until the required action is performed by the target user. Automatically generate email notifications for escalation if an application/ task exceeds defined processing time thresholds.	High	

S. No	High-level Functional Requirements	Priority	Response (Yes / No)
	Email alert contents and audiences should be user-defined.	Low	
25.	Data Control		
	Secure data by limiting changes by role, privileges, and status on the application.	Low	
26.	Audit Trail/Audit Logs		
	Audit Trails/logs should be available for all data input screens and approval processes. Audit logs should contain a field, screen/form level logs as well field level logs, and changelogs for document management utility. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
	Audit Trails/logs should be available for all processes, transactions, and Static Data updates (including user/role maintenance).	Low	
	Audit logs should contain screen/form level logs as well field level logs.	Low	
27.	Decision-Making through Smartphone		
	The system should be compatible enough to give a user-friendly interface on any Smart Mobile/Tablet-based browsers.	Low	
	Note: • There is no need to develop any separate Mobile App for the Corporate Loan Origination System. • The Loan Origination System (LOS) must be a web-based application, accessible and fully functional on mobile devices.		
28.	LogBook/Task Tracking Sheet		
	The system should have a feature to display the TTD/Task-In-Hands MIS to the user and its Reporting to users along with task details.	Low	
29.	User Manual, Help & FAQs		
	The system should have the feature that when the mouse hovers over any Tab/Accordion, it will be described as that item.	Low	
	Configuration Changes: In the configuration setup, the system will provide an option to update the description of that field. So, when the mouse hovers over any tab/Accordion, it will provide the description.	Low	
	The system should have built-in FAQ features for user support.	Low	
30.	Sanction Advice		
	System to generate sanction advice/CP snapshot with the relevant information only (i.e., Details of the obligor, facilities, collateral, pricing, Terms & conditions, exceptions, etc.) Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	

Technical Requirements

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
1.	Service Oriented Architecture (RESTful, SOAP Microservices)	High	
2.	Web-based solution.	High	
3.	The system should have a standard menu structure	High	
4.	User-friendly Graphical User Interface	High	
5.	Data Purging, Archiving & Data Warehouse Support	High	
6.	Supported file formats	High	
7.	Data Encryption & Security Support	High	
8.	Multi-Language, Multi entity, multi-currency	Low	
9.	Parameterization and Customization (Entire Application)	High	
10.	Business Process Management Capability/Integration	High	
11.	Compliance with Regulatory Requirements	High	
12.	Software Development Platform/IDE	High	
13.	Network related Requirements	High	
14.	Segregation of Functional and Security/ Admin modules	High	
15.	Big Data Integration	Low	
16.	Business Intelligence Capability	Low	
17.	Business Continuity and DR availability	High	
18.	Change, Patch & Release Management Process	High	
19.	Data Migration Techniques & Methodology	Low	
20.	Compliance with Regulatory Requirements	Low	
21.	Version Upgrades	Low	
22.	Single Sign-On (SSO) Support & Integration with Enterprise Identity and Access Management Solution	Low	
23.	Log Files & Audit Trail	High	
24.	Data Integration	High	
25.	Is it possible for a user to choose his or her role from a standard list of organizational roles specifically for the Loan Origination Module?	Low	
26.	Security standards should be implemented (code obfuscation, SSL pinning, and session hijacking refer to Open Web Application Security Project [OWASP] standards), and the platform should have the latest security features implemented.	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
27.	The platform should provide a Security Administration role that will only be used to perform security duties (e.g., event log auditing).	High	
28.	Minimum security requirements that the platform should support include (but are not limited to) the following: • Safety by design – implement the best security practices in solution design. • Support multifactor authentication and strong access control mechanisms. • Multi-tiered user and role management. Detailed list of software that needs to be licensed other than the proposed solution itself, such as Database, OS, Middleware, Connectors, etc.	High	
29.	Does the platform provide the authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials (SSO) feature for back-office users?	High	
30.	Is it possible to send an email, SMS, or print/publish report/daily stats or requests using your Platform?	High	
31.	Is it possible to apply the Security Model depending on role, user, and/or geography?	High	
32.	Is it possible to create and assign workflows based on the user, role, or geographic location?	High	
33.	Is the platform capable enough to display the error logs with their description to allow traceability of the data/function error to the most granular level?	High	
34.	Is the platform capable of handling file(s) attachments? What file kinds are supported, list them down here.	High	
35.	In terms of page structure, workflow and page flow, service connectivity, and business rule setup, the application can be configured to meet individual client requirements.	High	
36.	The platform shall provide a functionality for Geo tagging.	High	
37.	Geographic Limits based on Country & Bank Regions	High	
38.	Embedded Document Management System (DMS) or ability to integrate with Bank's existing DMS	High	
39.	The platform's APIs/Microservices should support custom Native apps or hybrid apps.	High	
40.	The platform should be compatible with the most recent server Operating System (OS) 2019 and above & web server.	High	
41.	The platform should support integration of mechanisms such as SOAP web service, RESTful web service, direct database, and so on.	High	
42.	Cross Browser Compatibility/ Browser versions supported?	High	
43.	The platform should support the Integration with various internal and external systems like CBA (Conventional & Islamic), eDMS, NADRA (BVS-Verisys), eCIB (direct or indirect), Tasdeeq,	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
	DataCheck, AML/Fraud System, Middleware (ESB/SOA), SafeWatch, Internal Blacklist, Anti Money Laundry, Multifactor Authentication Server, SMS Gateway, USSD Gateway (VRG), 1Link, NBP Email Exchange Server, Document Scanning (OCR capability would be required), HRMS, Employee Self-service Portal, 3rd party applications? This comprehensive integration support will ensure seamless communication and data exchange between the platform and these systems, enabling efficient and streamlined operations within NBP.		
44.	The platform must support XML, JAVA, MySQL, PostgreSQL, Oracle Database, Microsoft SQL Server, and Visual Studio ISO-based integration.	High	
45.	The platform must be compatible with third-party systems that DO NOT support open standards.	High	
46.	NBP has a presence in a variety of markets and geographies in the region, is it possible to aggregate customers into a single site or app using the Platform?	High	

Pre & Post Granting Applications/Activities

The system should enable configuration/changes in screen layouts and credit application report formats according to NBP's requirements.

Data captured on all input/decision screens should be printable as per credit application formats defined by users as per guiding source documents such as the National Bank of Pakistan credit policy manual. All users involved in the initiation/approval/processing of credit applications (with pre-assigned privileges) should be able to generate these reports as per allocated rights and privileges.

The system should be able to generate an Executive Summary, Economic Group Summary, and other credit application format reports based on data captured within the credit application. These reports should be configurable as per the National Bank of Pakistan Credit Manual Formats.

Note:

The National Bank of Pakistan uses a specified application format for different credit application types, which include but are not limited to the following types without any dependency on the Approved Credit Application in the LOS database.

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
1.	Borrower Credit Application - Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
2.	Temporary Release of Credit Documentation – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
3.	Permanent Release of Credit Documentation – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
4.	Document Deferral Memo – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
5.	Document Waiver Memo – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
6.	Temporary Extension Memo – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
7.	Classification Memorandum – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
8.	Classified Credit Review – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
9.	Watch Listing – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	

S. No	High-level Technical Requirements	Priority	Response (Yes / No)
10.	Relationship Transfer Memo (RTM) – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
11.	Excess Over Limit Memo – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
12.	Sub-allocation Memo – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
13.	Call Report – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
14.	Annual Renewal – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
15.	Interim Review – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
16.	Closure of Relationship – Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
17.	Restructuring & Rescheduling - Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	

Credit Monitoring (Loan Monitoring System – LMS)

Post Approval Documentation and DAC Issuance

The system should automate post-approval processes, including the generation of document checklists based on approved facilities, securities, and regulatory requirements. These checklists should be electronically circulated to relevant parties. The system should also generate standardized legal agreements and track document status, including logging observations and rectification actions. Additionally, the system should create customized offer letters based on approved facilities and implement a two-factor authorization process for disbursements.

Credit Monitoring/Maintenance

The system is expected to have a dedicated & comprehensive module for Credit Monitoring/Maintenance after the disbursement is made. The system should have the following functionalities:

Responses should be filled in as indicated below.

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	The system should have a Separate Pledge Accounting feature available.	High	
2.	Collateral Management of syndicated transactions.	Low	
3.	Monitoring of full scope & desktop valuation along with required details with the ability to record observations & condition of the built. The system should automatically generate alerts/reports for the expiry of the valuation. Such alert generation frequency should be customizable.	Low	
4.	Monitoring Insurance policies, premium payments (bullet/periodical), risk coverage, Co-Insurance arrangement, & Insurance Company per-party concentration limits.	Low	
5.	The LOS shall integrate with insurance providers, calculate premiums (including asset depreciation), and generate repayment schedules incorporating insurance costs. It shall replace the CBA for billing and accounting, effectively functioning as a comprehensive LMS.	Low	
6.	The system should also trigger alerts for stock inspection/joint stock inspection to be conducted before the dates they are falling due. The	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
	frequency of alert generation should be customizable.		
7.	The system should trigger automated alerts/reports to the relevant stakeholders for confirmation of the genuineness of Insurance policies.	Low	

Security/Collateral Handling

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	The system should be able to capture detailed information, specifically mentioning whether this is 1st Party Collateral/3rd Party collateral in listed categories of security/collateral. • Hypothecation of Current Assets, including stocks, receivables • Hypothecation of Plant & Machinery • Mortgages (Equitable, Registered & Token) • Fixed/Movable Assets • Lien over negotiable instruments/Accounts/PIBs/Bills of Exchange • Pledge of Shares • Pledge of Stocks • Vehicles • Guarantees (Corporate, Personal & GoP based Guarantees) • Any Negative Remarks by the Valuator? • Charge on Fixed Assets • Charge on Current Assets • Value of Shares Held as Collateral • No. of Days Collateral remained uninsured/underinsured.	High	
2.	The system should be able to record the allocation of pledge sites to the Muqaddam company.	Low	
3.	In this respect, the system should be able to record the ranking statuses of Hypothecation & Mortgage Charges registered with SECP. The	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
	system should also be able to manage third-party securities/collateral and should calculate the cushion requirement concerning total exposure secured against each security/collateral.		
4.	Under the security section, a section mentions how much security is complied with now.	Low	
5.	Collateral coverage in terms of %age of risk-based exposure.	High	
6.	Collateral details should have descriptive as well as absolute Values field/information as per SBP reporting Annexure-III requirement.	High	
7.	The system should have the ability to cater to multiple collateral tagging with a single facility & single collateral with multiple facilities. (Identification of Primary and Secondary Collateral).	High	
8.	The system should have the ability to capture and monitor the Exceptions.	High	
9.	The system should have a separate module for monitoring all collaterals (Collateral Charge, Component details, cash margin, coverage), Keeping Track of Group collateral information, Proper management, and correct regulatory reporting, Collateral Exception, Covenant tracking, Mark and reviewing Collateral Documents and their expiry dates along with its specific and comprehensive/dynamic workflow.	Low	
10.	Enable user to enlist/delist Valuator, muqaddam, and C&F Agent from LOS System, including uploading/downloading of required documents from the system.	Low	
11.	Enable users to update the list of active Muqaddams with their assigned limits.	Low	
12.	Extract report w.r.t number of pledge sites allocated to each muqaddam against total facility-wise limit.	Low	
13.	Extract region-wise concentration report of each Muqaddam	Low	
14.	The system should be able to trigger a guarantee expiry report, starting at least a month before actual maturity.	High	

S. No	Functional Requirements	Priority	Response (Yes / No)
15.	The system should generate automated triggers for the submission of periodic stock statements.	High	
16.	The system should have the ability to trigger alerts when stock inspections are due (or overdue) Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
17.	The system should provide for online submission of stock inspection reports.	Low	
18.	The system should allow users to capture different types of collateral values, such as Forced Values, Market Value, and Book Value, with valuation dates and Evaluator details. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
19.	The system should be able to maintain multiple charge types against collateral. Note: To demonstrate compliance with the specified requirement, please provide screenshots from the LOS System with corresponding page numbers included in the proposal.	High	
20.	The system should have the functionality to capture the details of Insurance, including co-insurance, risk types, premium amount, etc. The system should also trigger pop-ups where insurance arrangements are less./Underinsured.	Low	
21.	The system should be able to record safe-in/Safe-out details for all documents, whether "temporarily released" or "permanently released". This should be done under maker/checker authorization. For temporarily released documents, the system should generate alerts if	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
	the documents are not returned by the allowed date/time.		
22.	The system must be able to maintain lists of Valuation & Stocks Inspection Companies with their workable amounts, regions, panels, history of enlistments/delisting with other banks, ownership details & security amount held against each company.	Low	
23.	The system should have detailed complaints log/register with the history of warning letters issued & complaint resolution ratio. Upon delisting of any such company, the system should generate automated alerts/reports amongst the stakeholders for their current country-wide engagements/allocations with the existing portfolio.	Low	
24.	The system must be able to generate the alerts for the following: • CA Expiry/Due Date • Limit Expiry • Valuation Expiry • Insurance Expiry • Risk Triggers • Covenant Alert • Special Condition Alert • Stock Report Expiry • Insurance Policy/Cover Note validity. • Deferral Expiry • Guarantee Maturities	High	
25.	The system should also be able to maintain lists of Insurance/Takaful Companies of the bank's panel along with their per party/per risk limits, bank-wide/overall exposure, details for parent insurer, Monitoring of Insurance claims settlements/rejections & contact information for confirmation of the genuineness of Insurance policies.	Low	

Identity and Access Management (for User/Role Management)

The system should have prudent Identity & Access Management functionality. This functionality should contain: Responses should be filled in as indicated below.

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	Maker & Checker functionality All user and role management functionality should be performed under the four-eye principle, wherein the maker will execute/initiate any request, and the checker will approve the same.	High	
2.	Privileges for Identity & Access Management Team Responsibilities should be segregated by defining specific roles for teams with different responsibilities and roles. For all user and role maintenance-related tasks, a separate role should be available so that the team having such a role should be able to perform end-to-end tasks about user/role maintenance only. Besides, they should not be able to perform any business/transaction activity other than user/role maintenance.	Low	
3.	User/role maintenance-related logs and reports Comprehensive reports/logs should be available for periodical reviews. Logs and reports should be available to monitor: • User-based reports listing what roles are assigned to each user. • Roles-based reports enlist all users with the specific assigned role. • Report listing all privileges assigned to the specific role. • A report should be available to review all roles, along with the aggregate list of privileges assigned to each user. Privilege type should be specifically mentioned against each form, e.g., Create, Update, Delete, View, etc. • A user maintenance review report will be required. • Field-level logs will be required for monitoring every amendment in user/role maintenance.	Low	

Checklist for User ID & Role Management

Responses should be filled in as indicated below.

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	Are ADMIN IDs escrowed?	High	
2.	Are user IDs Locked by the application after non-usage of user ID as per IS Policy?	High	
3.	Is user password change enforced as per IS policy?	High	
4.	A newly created ID does not lock out after 07 days' non-usage (first login) of the User ID as per IS policy.	High	
5.	Are user IDs Locked by the application after three invalid login attempts?	High	
6.	One-Time Password: Does the application prompt for a change of password after the first login?	Low	
7.	Is user password complexity enforced/applied?	Low	
8.	Is a maker/checker available for user ID creation and amendments?	High	
9.	Is a separate role for user access management available & restricted to access management only?	High	
10.	Are audit logs and user modification logs available?	High	
11.	Is Access Rights Matrix available (please share)?	High	
12.	Is integration with Single Sign-On (SSO) available?	Low	
13.	Can an Identity & Access Management (IAM) user (with Role Change rights) assign roles to himself?	Low	
14.	Is the user ID Locked option available on the user ID amendment screen?	Low	
15.	Is a password reset option available in the end-user application?	Low	
16.	Is the Remarks/Description field available on user ID creation and amendment screens for user request reference?	Low	
17.	Is a user guide available for user access management (please share)?	Low	

Reporting – (High Requirement)

Users should be able to generate multiple reports, which include but are not limited to the following.

S. No	Name of the Reports	S. No	Name of the Reports
1.	Approval/Limit Expiry Report/CA Reviews	2.	Sugar & Rice Financing Report with DP Calculation
3.	Extensions allowed/Limits on Valid Extension	4.	Credit Maintenance Report – Complete
5.	Excess Over Limits/One-Offs	6.	Client/Facility Level ORR/FRR Report with Trend Analysis
7.	Sub-Allocation	8.	Segment-wise ORR
9.	DP Report	10.	FRR-wise Analysis
11.	Deferral Report (for valid and expired deferrals)	12.	GOV & GOP Backed Exposure Report
13.	Waiver/Deviation/Exceptions approved Report	14.	SBP - Industry Concentration Reports
15.	Approval Terms & conditions and Covenant Monitoring Report	16.	Pending DACs
17.	Valuation Report/Valuation Expiry	18.	Portfolio Report
19.	Insurance Report/Insurance Expiry	20.	Downgraded-Upgraded ORR
21.	Call Report/Missing Call Report	22.	PEP/Related Part/NAB Report
23.	Stock Report/Missing Stock Report	24.	Legal/IB Documents Expiry Report
25.	Stock Inspection report	26.	Industry-wise concentration limits, O/s, segment, region
27.	Missing Stock Inspection by RM	28.	Limits & Outstanding reports (on different parameters like Segment-wise, Customer-wise, etc.)
29.	Security-based reporting	30.	Expired Limits – Segment-wise (with number of A/Cs, outstanding, etc.)
31.	SME Advances, SME District wise, SME application details	32.	Missing Balance Sheets Report
33.	Large Exposure Customer	34.	Valid Term Loan not reviewed
35.	SBP Credit Review Inspection Report	36.	Credit Bureau
37.	Total Number of DACs issued by the Managers – CAD	38.	Non-financial approvals (Change of PGs, Amalgamation, Mergers, Acquisition of New Business, Sharing of Godown for Pledge Goods, etc.)
39.	Pre-Call Brief Report (NBP Specific).	40.	Types of Stocks under pledge report on a real-time basis along with associated Muqaddam
41.	Ear Marking of Limits	42.	Past Due Obligations (Days Past Due)
43.	Pending stocks report against Hypothecation and pledge financing.		
44.	The system should be able to generate eCIB-related reports by fetching data from the Core Bank System and other applications through direct or indirect integration with the eCIB portal or the bank's internal portal. This process must comply with the State Bank of Pakistan's regulatory policies in this perspective. The system should also be capable of automatic verification of extracted data on a pre-defined set of rules. This will encompass all periodic reporting to SBP, e.g., Settlement reports, etc.		

Obligor Reporting – (High Requirement)

The system should be able to generate detailed Obligor-related reports by fetching data from LOS, Core Bank System, and other applications through direct or indirect integration or the bank's internal portal. This process must comply with the State Bank of Pakistan's regulatory policies in this perspective.

Report Data Format:

Name of Group	Net Profit/(Loss) After Tax
Borrower's e-CIB Code	Equity
Name of Borrower	Change in Equity over last year
Borrower's Code (As per bank)	Surplus/(Deficit) on Revaluation of Assets Eligible for Equity
Sector	Subordinated Loans
Age of Relationship with Bank	Current Ratio
No. of years in Stated Business	Inventory Turnover Ratio
ORR on the Last inspection cut-off	Operating Profit Margin
Current ORR	Return on Assets
Overriding of ORR	Return on Equity
ORR By Audit/ BRR	Debt to equity
External Credit Rating	Interest Coverage Ratio
Total (fund and non-fund based) exposure at the start of the Inspection period	Debt Service Coverage ratio
Funded exposure as on Inspection Cut-off	Borrowing from Group Companies
Total (fund and non-fund based) exposure as on Inspection Cut-off	Lending to Group Companies
Is the Borrower a Related Party of the Bank	In the Case of the Individual Borrower, the Personal Net worth of the Individual.
Is Borrower a PEP?	Amount of GoP Guarantee
Annual Financial Cut-Off of the Borrower	Mortgage
Latest Audited Financials published/ issued by the borrower?	Any Negative Remarks by the Valuator?
Cut-off of Latest Financials Available with Bank	Charge on Fixed Assets
Name of External Auditor	Amount of Charge
Qualification/ Emphasis of matter (If Any)	Value of Security (if different from balance sheet amount)
Growth/(Decline) in Sales over the last financial year	Charge on Current Assets
Gross Profit/(Loss)	Value of Shares Held as Collateral
Net Profit/(Loss) Before Tax	No. of Days Collateral remained uninsured/underinsured
Growth/ (Decline) in Profit Before Tax over last year	Case registered/ pending with FIA/ NAB, if any

Facility Reporting – (High Requirement)

The system should be able to generate detailed Facility-related reports by fetching data from LOS, Core Bank System, and other applications through direct or indirect integration or the bank's internal portal. This process must comply with the State Bank of Pakistan's regulatory policies in this perspective.

Report Data Format:

Branch Name	Repayment tenure after R & R
Branch Code	DPD at the time of RR
Name of Group	Deferment of Current accrued Mark-up (Fully or Partially)
Borrower's e-CIB Code	Waiver of overdue or Current Mark-Up
Name of Borrower	Number of Deviations/ Exemptions/ Exceptions of Bank's Own Policy
Loan Account No	No. of Regulatory Exemptions/ Exceptions/ deviations obtained from SBP
Sub-Facility Number	During the Inspection Period
Funded/non-funded	As on Inspection Cut-off
Type	Account Behavior in WORKING CAPITAL FINANCE
Purpose of Loan Facility	Annual cleaning in the last year of the loan
Date of e-CIB obtained at the time of approval	No. of Days of Clean-up
Date of BBFS Obtained by Bank	Debit Turnover last year of the loan
Date of Approval	Credit Turnover last year of the loan
Approval Authority	Deferrals/Exemptions/Exceptions in Collateral
Date of Disbursement	No. of Times Deferrals allowed in security perfection.
Approval Type	List of exemptions/ exceptions/ Deferrals in collateral as of inspection cut-off
Facility Risk Rating (FRR)	List of exemptions/ exceptions/ Deferrals in collateral waived after approval.
Forced Conversion from non-funded to funded?	Secured/ Unsecured
Main Limit/Sub-Limit	Collateral Type
Amount	Amount of Cash /Liquid Collateral
Date of Expiry of Limit	Pledge (Commodities)
No. of Limit Enhancements	Name of Commodity
No. of One-off approvals	Total Amount
No. of Temporary Extension	Replenishment of Stock
No. of Times Excess over the limit was allowed	No. of Stock Visits
Outstanding as of inspection cutoff date	Shares Held as Collateral
Days Past Due as of Inspection Cut-off	Total Value
Principal	Margin maintained
Mark-up	Includes third-party shares without a pledge mandate?
Present Classification Category by Bank	Changes in Collateral
No. of Times Principal Repayment was delayed During the Inspection Period.	Was any security released during the inspection period?
DPDs 80-90	Was collateral changed during the inspection period?
DPDs 90+	The cumulative Number of days shortfall occurred During the Inspection Period in
No. of Times Mark-up payment was delayed During the Inspection Period	Security
DPDs 80-90	Margin
DPDs 90+	Amount of Shortfall as Inspection Cut-Off
No. of Restructuring & Rescheduling	Security
Repayment Tenure before R&R	Margin

Number of Restructurings/Rescheduling during the Inspection Period	Name of Insurer
DPDS at the time of Rescheduling/Restructuring - Principal	Date of premium paid receipt for current year
DPDS at the time of Rescheduling/Restructuring - Markup	No. of month assets remain uninsured during the inspection period
Any enhancement in limit at the time of restructuring	Number of inspections
Deferment in Markup (accrued/ current) at the time of Rescheduling/ Restructuring	Negative observations in stock inspections (if any)
Classification Category Before Rescheduling/ Restructuring	Was this facility converted from Short Term to Long Term and Vice Versa
Classification Category after Rescheduling/ Restructuring	Date of Conversion
As per the Bank's Own Policy (Outstanding as of cut-off date)	Number of times excess over limit obtained during the inspection period
Regulatory Exceptions During the Tenure	Was an excess over limit converted to the regular limit of this facility?
Regulatory Exceptions as on Inspection Cut-off	Date of conversion of the excess over the limit into a regular limit (if any)
Excess over limit outstanding as of Inspection Cut-off Date	

User Entitlement Report – (High Requirement)

User maintenance reports will be required for periodical reviews, in addition to other fields, the following are the minimum requirements:

S. No	Report Details	S. No	Report Details
1.	User ID	2.	Assigned Branches/Regions
3.	Username	4.	Assigned Business Segments
5.	Employee ID	6.	Last Login Date
7.	Branch	8.	Login Attempt Allowed
9.	Department	10.	Login Attempt Made
11.	Designation	12.	Last Password Change Date
13.	Role/Group	14.	Password Expiry Date
15.	Email ID	16.	User Created on Date
17.	Rights against roles	18.	User ID Update Date
19.	Employee ID	20.	User ID Created by Employee Number
21.	Status	22.	User ID Created by Employee Name
23.	Back-up Employee	24.	User ID Updated by Employee Number
25.	Reported To	26.	User ID Updated by Employee Name

General Requirements

Responses should be filled in as indicated below.

Yes – Standard Feature (fully compliant)

No – Feature not available.

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	The system should be compliant with the State Bank of Pakistan's regulatory policies, both functional and technical.	High	
2.	The system should be compliant with standard Information Security Requirements as specified by the Bank's IS function from time to time.	High	
3.	The system should offer the "Forgot Password" option so that the user can generate a new password without reference to the "Identity & Access Management" team.	Low	
4.	As the system is to be used in Pakistan and its international regions, hence a user should be able to access the system from all locations. i.e., If an approval authority, designated in Pakistan, visits any international region, he/she should be able to access and use the system without interruption. Simultaneously, a user of any international region should be able to access the system from the bank's premises within Pakistan.	Low	
5.	The System is to have integration support available to fetch customer information (CIF details) from the Core Bank System. The system will always pull such data from the Core Banking System and will never push client information to the Core Banking Application.	Low	
6.	Parameterization: The system should be highly parameterized to add any change in: a. Approval matrix/business process flow at the run with ensuring uninterrupted flow/execution. b. Approval Matrix update/Create rules and matrices with breakthrough ease. c. Approval authorities update recommenders and approvers. d. Parameterized Product Structure Management/Product Management e. Business Hierarchy/Role Hierarchy Management f. Static Data update for all functionalities g. Filed addition in forms/screens on a need basis	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
7.	System to allow all such changes to be incorporated by the bank's user from UI without vendor engagement.	Low	
8.	System to control data access using roles and authorization overrides.	Low	
9.	The system should be able to migrate data from legacy applications to another new platform.	Low	
10.	Escrow arrangements for software/source code.	High	
11.	Knowledge transfer to NBP's team for incorporating necessary changes in the system to cater to future requirements.	High	
12.	Experience of the Bidder: The Bidder must demonstrate a proven track record of successful Corporate Loan Origination System (LOS) deployments and implementations. Specific Requirements: Minimum of one (1) successful Corporate LOS implementation in Pakistan (Commercial Bank). Comprehensive Documentation: Provide evidence such as signed purchase orders, work orders, agreements, and client references to substantiate the claimed experience. Unverified Documentation: Unsigned and unstamped documents will not be considered. Evaluation Criteria: All credentials and other evaluation criteria will be assessed as of the RFP closing date, excluding financial information.	High	
13.	The bidder will be responsible for the complete implementation of the proposed solution. The bidder must also ensure and confirm that the quoted price is in line with the standard rates in the market. Note: Bidder is to provide acknowledgment/ undertaking for this requirement on company letterhead with proper reference (page No) in the proposal.	High	
14.	Warranty, Support, and Maintenance (24x7x365) of the Proposed Solution.	High	

S. No	Functional Requirements	Priority	Response (Yes / No)
15.	Bidder must provide comprehensive support offerings, including Phone Support, Email Support, and an Online customer portal to access patches, upgrades, new version support, and via online download or other methods. Note: Bidder is to provide acknowledgment/ undertaking for this requirement on company letterhead with proper reference (page No) in the proposal.	High	
16.	Propose a Project Manager who will be assigned to manage this project from beginning to end. The Project Manager must have at least ten (10) years of relevant experience in managing similar projects. Identify another key member of the project team who will be assigned to work on the project, whether the member will work on-site, including all designers, coders, documenters, management, and support staff. Please use the template in '*Annexure-3*' to provide the resumes of the Project Manager and other key members of the team.	High	
17.	Bidder should submit details of the team that would be responsible for designing, development, customization, integration, implementation, User Acceptance Testing, Training, Operations, and Maintenance phases of LOS. Bidder must ensure that end-to-end Solution Implementation phases are led by a Subject Matter Expert. The proposed team for Solution Implementation must comprise at least three resources and have experience in executing LOS projects. CVs/Resumes, along with professional certificates (if any), shall be submitted. Note: Bidder is to provide acknowledgment/ undertaking for this requirement on company letterhead with proper reference (page No) in the proposal.	High	
18.	Bidder may involve the NBP team during the deployment and implementation phase and pass on the complete configuration document after implementation. Bidder to provide acknowledgment/ undertaking for this requirement.	Low	

S. No	Functional Requirements	Priority	Response (Yes / No)
	Note: Bidder is to provide acknowledgment/ undertaking for this requirement on company letterhead with proper reference (page No) in the proposal.		
19.	Proposed Solution Testing Requirements: Bidder must provide complete on-site support during the entire NBP testing exercise of the Proposed Solution (i.e., before Go-Live). The undertaking shall be provided by the bidder on the company's letterhead. Bidder shall provide a user acceptance testing (UAT) methodology for the testing of the Proposed Solution, including the bug-fixing process.	High	
20.	The bidder would develop and arrange a testing methodology for the testing of the provided capacity benchmark/metrics of the proposed solution through manual input and Simulators in coordination with NBP after being awarded the contract. NBP will perform testing of the solution after its deployment through manual input, and branch mark/load testing will be performed using a simulator provided by the bidder. The bidder should undertake that any gaps found therein would be fixed by the bidder without any additional cost.	High	
21.	Bidder should provide an undertaking that it will provide full support in remediating and fixing all issues that will be reported by third-party companies during the Penetration Testing/Ethical Hacking/Web Vulnerability assessment of the proposed system. This exercise will be performed before the Go-Live phase.	High	

S. No	Requirements	Response
1.	Describe in detail the scalability features of the platform.	
2.	Details of the Security Model Used by the Platform for Protecting the NBP and its Customers.	
3.	How does your Platform manage user profiles and group management?	
4.	What is the Language platform used to develop the solution? e.g., JAVA, .net, node JS, python, etc.	
5.	What is the development methodology?	
6.	What are the supported Application Server Platforms?	
7.	What are the front-end Frameworks?	

8.	What is the minimum hardware requirement? Keeping in view the number of Users (1,500), Corporate Credit Proposal Volume (+ 50,000)? Note: Attach the separate annexure with detailed Hardware Requirements within the Bill of Quantity (Section X). Recommend the detailed infrastructure with specifications required for rolling out the solution, including (but not limited to) hardware, Operating System, database, middleware, replication technologies/tools, version management tools, software licenses, and support subscription.	
9.	What is the LOS Platform Architecture and Components Diagram (with/without high availability) and disaster recovery (DR) sites	
10.	What are the other pre-built integration components supplied with the platform?	
11.	Provide details on the platform's integration with the bank's legacy system or third-party fintech and aggregators.	

Standard Functionalities

This system should provide the following functionalities as a part of the CLOS:

S. No	Functional Requirements	Priority	Response (Yes / No)
1.	Realtime TAT Monitoring (User wise, Profile wise & Segment wise)	High	
2.	Email Alerts and Notifications	High	
3.	SLAs & Auto Escalations Matrix	High	
4.	Business Segment Shuffle/Portfolio Shuffle	Low	
5.	RM/ARM/AFO Portfolio Shuffle	Low	
6.	Leave Marking & Unmarking	Low	
7.	User Bucket/Authority Swap (Vertical & Horizontal)	Low	
8.	Customized Reporting and Dashboards	High	
9.	Error Handling (Generic Functionality)	Low	
10.	Segment/User Profile wise Tab Linkage	Low	
11.	Business Segment wise Field Level Linkage	Low	
12.	Group Chat	Low	

Information Security-Related Requirements

Application Security Review Checklist

Application Security Review Checklist

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
1.0	Application Components	Acceptable Criteria	
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 define 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 usernames.	
2.6	Initial Password Does the application prompt to change the initial password?	Default passwords are changed following installation of system or software. Initial password should be pre-expired. Application should immediately prompt to change the initial password upon users first log into the application. Applications are configured to enforce password change upon first login whenever temporary password is issued (e.g., account re-activation after account lock out, or password reset request, etc.). In all cases, user authentication should be ensured, either by asking old password or by sending reset link to registered email address, etc.	
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 disabled autocomplete	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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: i. Password history should be maintained for at least 6 passwords. ii. 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 username etc. iii. Password must be Alpha-Numeric with both upper and lower case characters (e.g., a-z, A-Z) iv. Password change interval must not be less than one (1) day. v. Must have at-least one numeric and one special character e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) vi. Account should be locked after 5 unsuccessful login attempts, and should only be unlocked upon receipt of request from valid user to the administrator or 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. Privilege Level • Minimum 12 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 username 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 username Password should not be easily guessable passwords e.g. 12345678, asdfasdf, etc. Password should not be blank. Static passwords must never be displayed on the screen in clear text.	
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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
		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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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. Application forcefully terminates all existing session when the user logs out and/or web browser is closed without logout. After successful logout from the application: All Session parameters on client side and server side should be removed. Application should not resume the session upon manual redirection to previous page. Application should not allow the cached version of authenticated pages.	
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 show by the application	
3.3	Entitlement Review report Does the application provides the complete details of all user's entitlement in form of a report? Security Administrator should have the ability to generate these reports per	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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
	department / unit for periodic user entitlement review.	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. User and Access Management should be independent, not managed by the same team who is performing business operations/tasks in the application.	
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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 usernames 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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
		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 including data in logs and data in backups (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. Special characters should not be allowed as input. If needed, whitelist the characters which can be accepted.	
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 in place 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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/requirement, 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 preventing unauthorized access.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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, Default application/DB/OS accounts should be identified and disabled where possible. If cannot disabled, default password should be changed with whitelisting and also define the ownership of these accounts. Service/functional accounts should be identified and their purpose shall be documented and approved by the relevant senior management along with the defined ownership and protection of credentials in storage and transmission. Service accounts should not have interactive login rights unless there is a valid business or technical need. Passwords for service/admin accounts should be in dual controlled as split knowledge and escrowed or managed via privileged id management solution. Password of these accounts should be more complex.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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. Access to audit logs including administrative activities is restricted for access. Audit logs should be protected against data tempering and un-authorized access. Credentials, PAN, PII, PIN block, etc. must not be the part of logs in plain text.	
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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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. Default application/DB/OS accounts should be identified and disabled where possible. If cannot disabled, default password should be changed with whitelisting and also define the ownership of these accounts. Service/functional accounts should be identified, and their purpose shall be documented and approved by the relevant senior management along with the defined ownership and protection of credentials in storage and transmission. Passwords for service/admin accounts should be in dual controlled as split knowledge and escrowed or managed via privileged id management solution. Password of these accounts should be more complex.	
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. Service accounts should not have interactive login rights.	
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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 Idle session timeout in applications is set to 5 to 15 minutes, based on asset classification.	
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. Authentication session ID should be changed upon each login.	
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 to 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;	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
		• 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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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 in config file. It should not be hardcoded. 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	If there is a need to support banner tax, legal-approved banner text must be displayed at all entry points where	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
	application, displayed at all entry points where a user initially signs on?	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 Information 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,	No default ID should be used or enabled. Default IDs should be renamed and password split and escrowed with IS	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
	disabled or protected to prevent their unauthorized use?		
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+.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design, and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop-down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
14.2	Have any non-compliance been 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 Application Security

Web Secure Coding Checklist		
The ITPM should complete this checklist with the project's developers in order to ensure compliance. This reflects best industry practice and correlates directly to issues that are identified during Vulnerability Assessments.		Answer (True, False, N/A)
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. user authentication should be ensured, either by asking old password or by sending reset link to registered email address, etc.	
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 Or when password is changed.	
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 upon each login.	
3.8	The session id is changed upon 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 "HTTP Only".	

3.14	Verify that authenticated session tokens using cookies are protected with the "secure" attribute and 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. Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.	
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) 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 account Balance, 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) 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 escaped properly.	
6.5	All untrusted data that are output to XML,LDAP,OS use parameterized interfaces or escaped properly.	
6.6	All untrusted data that are output to any interpreters not specifically listed above 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. Encrypt all data in transit with secure protocols such as TLS with forward secrecy (FS) ciphers,	
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 invalidated 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 HTTP Only 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

API Security Review Checklist

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
1.0	Authentication & Authorization	Acceptable Criteria	
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 Authority 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 instead 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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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-URL encoded, 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 decency 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.	

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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: Same origin (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	• Eternal entities' 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		

INSTRUCTIONS: To be completed by the Project Manager, developer, and ISO during the Definition, Technical Design and Validation Project Phases, except where noted as not required. Fill in all applicable sections. Use drop down menus where available. Insert N/A as appropriate.		Guide	Answer (True, False, N/A)
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.	

Database Security

Database Security Controls Requirements

<table>
<tr><th colspan="2">Vendor to share technical documents/evidence/responses for the following database security controls requirements:</th></tr>
<tr><td>1</td><td>The database solution offered by the vendor must support password configuration/control parameters for database privilege / named users which at a minimum includes:

Minimum Length
• The password must be a of minimum eight characters in length for standard user IDs and twelve characters for administrative/privilege IDs.
Complexity:
• Must be Alpha-Numeric with both upper and lower case characters (e.g., a-z, A-Z)
• Must have at-least one numeric and one special character e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
History.
Same password was not used within at-least the last 6 changes.
Account Lockout
Password must be locked out after 5 failed login attempts.
Password Expiry
Passwords are forced to be changed after 1 month.
The database must have capability to change passwords of default and unused database accounts.</td></tr>
<tr><td>2</td><td>The database solution 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.</td></tr>
<tr><td>3</td><td>The database must provide best-practice security configuration as per industry leading compliance standards, such as CIS benchmarks.</td></tr>
<tr><td>4</td><td>The database platform must provide native capability of data encryption to protect customer PII / confidential data stored in back office database tables. 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. Vendor also required to share technical documents / evidence pertaining DB encryption standard and process for secure management of DB encryption keys.</td></tr>
</table>

Vendor to share technical documents/evidence/responses for the following database security controls requirements:	
5	The database should provide native capability of data redaction/masking to protect customer PII data / confidential data on test database environment. In addition, Database should be flexible to support integration with any 3rd party data masking/redaction solutions.
6	The database should provide role-based-access control at the granular level and allow database administrator to centrally manage roles and privileges of database users.

Infrastructure Security

- The solution must be compatible with OS CIS controls (Linux/Microsoft).

Project Team Members' Resumes

Resume Format

Please provide a proposal following the details mentioned in "Annexure-3".

Name of the Person:	
Title:	
Years with the Firm:	Core Expertise:
Education/Qualifications: (Summarize college/university and other specialized education, including school names, dates of attendance, and degrees, certifications, and professional credentials attained.)	
Employment Record: (Begin with your current position and work your way backward through your relevant work experience.) Give dates, names of employers, titles of roles held, and location of employment for the last ten (10) years.)	
Experience: (Detail the sorts of activities performed, degree of responsibilities, location of assignments, and any other information or professional experience relevant to this project for the last ten (10) years.)	

I, the undersigned, certify to the best of my knowledge and belief, that this bio data is accurate and confirms my availability.

________________________________ ____________________

Signature of Personnel or Firm Representative Date (Month/ Day/Year)

Client Reference Details Format

Please provide a proposal following the details mentioned in this "Annexure-4".

Name of the Bidder: ____

Name of Organization and its Address:	
Name and Title of Point of Contact: (provide 2)	1. Sample 2. Sample
Telephone Number:	
Email Address:	
Period of Performance:	
The location where project services were performed:	
Description of Products Services and their relevance to the requirements under this RFP	

8. Technical Evaluation Criteria (Section-VIII)

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

1. All bidders are required to submit filled, correct, and complete SPECIFICATIONS/REQUIREMENTS (SECTION VII). If the bidder fails to do so, its bid will be considered rejected.

2. All bidders are also requested to affix their company's stamp and signature on each page of the submitted SBD. If the bidder fails to do so, its bid will be considered rejected.

3. All bidders are required to propose a single solution brand/model/latest version OR subsequent upgraded to NBP as any other alternate or additional brands/models will not be considered for evaluation, and such bid will be considered as rejected. Only upgraded models will be acceptable at the time of delivery. This clause will serve as a floor.

4. If any bidder includes proposed solution financial details (i.e., price, cost, bid security amount, etc.) in its TECHNICAL PROPOSAL or response to any NBP clarification query during the evaluation of the technical proposal, its bid will be considered rejected.

5. The evaluation of solution functional requirements mentioned in SPECIFICATIONS/REQUIREMENTS (SECTION-VII) with **"Priority (High/Low)"** is evaluated as follows:

   a. For evaluation purposes, a desired response of only "Y"/ "Yes" or "N"/ "No" is required in the availability column for all technical requirements (mentioned in SPECIFICATIONS/REQUIREMENTS (SECTION-VII).
   b. All technical requirements with "High" Priority must be answered as "Y" or 'Yes.' If the bidder responds 'N' or 'No' against any of such "High" Priority requirements, its bid will be considered as technically disqualified and will be rejected.
   c. All technical requirements with 'Low' Priority can be answered as 'Y,' 'Yes,' 'N,' and 'No' as these requirements will not be considered for evaluation. If the bidder responds 'N' or 'No' against any of the "Low" Priority requirements, its bid will not be considered as rejected.
   d. For all 'High' priority technical requirements against which Bidder is responding "Y," the bidder should specify the proper reference of the proposal in the reference/substantiation column. NBP may ask for any other additional documentary evidence against any requirement that must be provided by the Bidder during the period of evaluation. Bidders should respond to such requests within the timeframe indicated in the letter/e-mail seeking the explanation. Failing to provide the reference, its bid will be considered as technically disqualified and will be rejected.
   e. 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 a reference document is found, then NBP asks for clarification from the bidder about its response, however, if the reference document is also not found, then the response of the bidder shall be considered as 'No', and its bid will be considered as rejected.
   f. 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 the financial proposal will be considered as final and cannot be varied in any case after the submission of the bid.
   g. 'Low' priority requirements that shall be responded to 'Y' by the bidder shall be treated as complimentary, without any addition to the above-mentioned quoted price.

6. Relevant evidence/reference must be provided in the technical proposal with complete reference/ page no, and if the evidence is not provided, the proposal will be rejected.

   a. If a bidder's response against any requirement is not available, it will be evaluated as a requirement 'Not' met and will lead to disqualification/ rejection of the bid.

   b. For all 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, and It is mandatory to provide proper references to the document. It is NBP's discretion to raise clarification queries against requirements where reference is provided and further clarification is required. In case no reference is available, and documents are not available in the submitted proposal, NBP may not raise any clarification query, and the response will be considered as NIL or No, which may lead to disqualification if mentioned in the criteria.

   c. NBP may ask for 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 timeframe indicated in the correspondence (letter/ e-mail). If the bidder fails to provide the required information within the given timeframe, its bid will be considered rejected.

   d. Qualification Criteria mentioned in SPECIFICATIONS/REQUIREMENTS (SECTION-VII) "Priority (High/Low)" is evaluated as follows:

      - Qualification requirements with "High" Priority must be answered as 'Y' or 'N.' If the bidder responds 'N' against any of such "High" Priority requirements, its bid will be considered as technically disqualified and will be rejected.

      - For "Low," Priority can be answered as 'Y,' 'Yes,' 'N,' and 'No'. If a bidder responds 'N' or 'No' against any of the "Low" Priority requirements, its bid will not be considered as rejected.

      - For all Bidder qualification 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 a reference document is found, then NBP may ask for clarification from the bidder about its response, however, if a reference document is also not found or provided, then the response of the bidder shall be considered as 'No,' and its bid will be considered as rejected if the requirement item is a high priority.

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

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

7. Financial proposals will be opened only to technically qualified bidders. Technically, unqualified bidders will be considered disqualified, and their financial proposals will be returned unopened.

8. The Bidders must include the price of all requirements with their Financial Proposal, as the price mentioned in the Financial Proposal will be considered final and cannot be changed under any circumstances after the

submission of the bid.

9. The prices will be evaluated based on all items mentioned in SPECIFICATIONS/REQUIREMENTS (SECTION-VII) of the RFP documents, which will be considered as total bid value/bid amount/contract price.

10. A combined evaluation of technical and financial proposals shall follow, and the bidder with the winning proposal will be accepted and considered as the **"Lowest Evaluated Bid"** and will be accepted for contract award.)

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

8.1 Financial Bid Evaluation

The Financial Offer should comprehensively detail all relevant price information for the **On-Premises** implementation model.

The following Items must be included:

- Retail/Consumer Loan Origination, Monitoring System/Collection and Recovery Module (Admin module included)
- Corporate Loan Origination, Monitoring System (Admin module included)

The financial details provided must align harmoniously with the Technical Offer and should explicitly exclude any hidden costs or undisclosed fees for quoted items.

All pricing information must be quoted in Pakistani Rupees, inclusive of all taxes, duties, levies, and associated costs. The Bidder is solely responsible for the accuracy of all calculations. NBP will not be held accountable for any errors.

The Bidder must guarantee the accuracy and validity of their calculations throughout the contract term. Any adjustments or appeals based on prior assumptions will not be considered.

The Bidder must demonstrate the financial capacity to successfully implement the LOS solution and provide ongoing management services as outlined in the contract.

If, for some reason, the successful bidder fails to execute an agreement within a specified timeline, the bank reserves the right to award the contract to the next most eligible and advantageous bidder based on the final evaluation scope of technical evaluation scores and financial prices quoted.

The Financial Proposal shall be provided as per the following layout:

On-Premise Component

The following components should be included in the pricing:

Component	Description
Software License Cost	The cost of licenses for the complete proposed solution, including all modules, is outlined in Section VII: Technical Requirements. The licensing model can be a one-time perpetual license, a recurring subscription-based license, or a combination of both.
Professional Services Cost	Costs for installation, configuration, and customization. Outline the scope of implementation services and associated costs. User & Technical Training of the Proposed Solution and all its modules for NBP's employees Cost for the on-site resident engineer till the completion of the scope of the project. Costs associated with travel and expenses of the staff. Include estimated costs for travel, accommodation, and other expenses.

Component	Description
	Fees for ongoing support, maintenance, and security updates. Detail the support levels, response times, and maintenance activities included, along with their costs.
Software Support & Maintenance Cost	Fees for ongoing support, maintenance, and security updates. Detail the support levels, response times, and maintenance activities included, along with their costs.

9. Payment Terms & Conditions (Section-IX)

1. In the event the contract is extended, it may be extended to up to 5 years. In this case, the Annual Cost of Three years of software, hardware warranty support & maintenance will be valid for 4th and 5th years upon renewal of the Support & Maintenance Agreement. Bidder will have to execute a software, support, and maintenance contract valid for three years from the completion of the month's onsite support period. The contract will be subject to renewal for the 4th and 5th years if the NBP decides to renew.
2. The total Bid amount must be inclusive of all applicable taxes. Any other associated cost should be mentioned explicitly by the bidder. NBP will not be responsible for any additional cost during the contract period for compliance with RFP requirements.
3. Bidders should provide the prices in Pakistan Rupees (PKR). The price quoted should be fixed and valid for a bid validity period (i.e., 270 days). If any bidder quotes the bid prices other than Pak Rupees, then for comparison and evaluation of bids, the price shall be converted into Pak Rupees. The rate of exchange shall be the selling rate prevailing on the date of opening of bids specified in the bidding documents, as notified by the State Bank of Pakistan / National Bank of Pakistan on that day.
4. NBP will make all payments in Pakistan Rupees (PKR) only.
5. Bidder is required to provide details of all other Software and accessories/hardware (if any) that are necessary for the proper and smooth working of the complete solution separately in the proposal as per the requirements mentioned in Section VII, and all such costs should also be included in its financial proposal.
6. Any enhancement in the solution within the contract period will be done by the successful bidder. The bidder will be required to submit the proposal for additional services at the time of request from NBP.
7. Bidder is required to provide details of all hardware details (Primary as well as Dev, UAT, SIT, and DR) which are necessary for the proper and smooth working of the complete solution separately in the proposal as per the requirements mentioned in technical specification.
8. The National Bank of Pakistan reserves the right to require the development or implementation of any requirements initially categorized as "Low Priority" during the contract term.

9. Bidders shall incorporate the potential development or implementation of all 'Low' Priority Requirements into their pricing proposals.

10. No additional fees or charges will be applicable for the development or implementation of any 'Low Priority' Requirements as specified by the NBP within the RFP/Scope and duration of this contract.

11. Within 30 calendar days after the signing of the contract, the successful bidder is required to submit a Performance Security, which shall be five (05%) 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 Pakistan Rupees (PKR). Discharge of the Performance Security shall take place; place after submission of a written request by the vendor within thirty (30) days after the Go-Live completion certificate issuance by NBP DBG. Submission of incomplete Performance Guarantee and/or fake Bank Guarantee will lead to immediate disqualification of the successful bidder, and NBP will pursue to blacklist the company as per Public Procurement Rules, 2004.

The payment terms and schedule for this implementation will be as follows:

Cost of Software Licenses

Payment Milestone	Payment Milestone Description	Payment Milestone Deliverables
35% upon Completion of the Project Initiation Phase.	This milestone will be reached upon the successful completion of the requirement analysis phase.	• Submission of the detailed project plan and hardware software requirements • Project kick-off meeting and team mobilization
65% upon Completion of the User Acceptance Testing (UAT) Phase.	This milestone will be reached when the vendor has completed the user acceptance testing of the loan origination system. The vendor will be required to submit a detailed user acceptance test plan, user stories, and test results for the National Bank of Pakistan's review and approval.	• UAT Sign-off

Cost of Professional Services

Payment Milestone	Payment Milestone Description	Payment Milestone Deliverables
10% upon completion of the project initiation phase	This milestone will be reached upon the successful completion of the project analysis phase.	• Submission and approval of detailed project plan and hardware software requirements. • Project kick-off meeting and team mobilization.
10% upon completion of the requirement analysis phase	This milestone will be reached upon the successful completion and NBP sign-off of the requirements analysis phase.	• Software Requirement Specification (SRS) Review and Sign-off • Business Requirement Document (BRD) Review and sign-off • Functional Specification Document (FSD) Review and sign-off
20% upon Completion of the Designing Phase and Development Phase	This milestone will be reached when the vendor has completed the design and development of the loan origination system, including all of the required features and functionality mentioned in BRD. The vendor will be required to submit a working	• Installable Media for complete Solution (Executable Code for Proposed Solution and all its Modules as mentioned in Section VII Technical Requirements) • Product Complete Technical & User level Documentation (For example, Software Requirement Specifications, Design Document,

Payment Milestone	Payment Milestone Description	Payment Milestone Deliverables
	prototype of the system for the National Bank of Pakistan's review and approval.	Database ERD, Installation Guide, etc.), User Manual, and Train the Trainer Manual. • Deployment of the system on the UAT Environment
10% upon Completion of System Integration Testing (SIT) Phase	This milestone will be reached when the vendor has completed the testing and integration of the loan origination system with the National Bank of Pakistan's existing IT infrastructure. The vendor will be required to submit a detailed test plan and test results for the National Bank of Pakistan's review and approval.	• SIT Sign-off
20% upon Completion of User Acceptance Testing (UAT) Phase	This milestone will be reached when the vendor has completed the user acceptance testing of the loan origination system. The vendor will be required to submit a detailed user acceptance test plan, user stories, and test results for the National Bank of Pakistan's review and approval.	• UAT Sign-off
20% upon Completion of the Go-Live Phase	This milestone will be reached when the vendor has deployed the system to the National Bank of Pakistan's production environment after IS review, which includes all modules/MVPs that cover the entire scope of the contract.	Deployment of the system on Production and DR Environments
10% upon Completion of The Go Live Phase	This milestone will be reached once the 6 month warranty period is completed.	Certificate of Completion of 6 Months Post-Go-Live

Cost of Support & Maintenance Services

Payment Milestone	Payment Milestone Description	Payment Milestone Deliverables
100% upon Completion of Post Go Live Phase	This milestone will be reached once the 6-month warranty period is completed. During this phase, the resident engineer is required to be on site.	Certificate of Completion of 6 Months Post-Go-Live of Entire Module.

Other Terms & Conditions

- All payments will be made in Pakistani Rupees (PKR) by transfer to the vendor's bank account or issuance of payment order in favor of the vendor.
- The vendor must submit a detailed payment schedule based on the milestones above (modules [RLOS & CLOS separately] and MVP-wise), along with their proposal. The payment schedule should specify the amount of each payment and the due date for each payment.
- NBP will procure all necessary hardware and software independently. Therefore, pricing for hardware and software should not be included in the bidder's response to this LOS-RFP.
- The vendor must also submit a copy of their banking information, including their bank name, account number/IBAN, and SWIFT code.
- The National Bank of Pakistan reserves the right to withhold any payments if the vendor fails to meet the agreed-upon milestones or if the system does not meet the required specifications as per the scope defined.
- The Vendor shall keep confidential all information disclosed by NBP in connection with this RFP.
- The Vendor shall be solely responsible for all costs and expenses associated with the project, including but not limited to personnel, software, licenses, and travel.
- The National Bank of Pakistan also reserves the right to make deductions from payments if the vendor fails to meet any of the other terms and conditions of the contract.

10. Bill of Quantity (BOQ) (Section-X)

Item(s)	Quantity
Licenses of Complete Proposed Solution (RLOS and CLOS seperatly), and all its Modules as mentioned in Section VII Technical Requirements **Note:** Including all PR, DR, SIT, and UAT servers	**For Corporate LOS:** Based on Users (1,500), Corporate Credit Proposal Volume (+ 50,000) **For Retail LOS:** Based on Retail Users (3,000), Retail Credit Proposal Volume (+ 300,000)
Cost of professional services	As required throughout the contract Period
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 Years [Also Valid for 4 or 5 years upon renewal by the NBP]
Provide details of all other Software (OS, DB etc.) and accessories/hardware (Cores, RAM, etc.) that are necessary for the proper and smooth working of the complete solution separately in the proposal.	As per the requirements mentioned in Section VII.
Local Training of 50 NBP Employees (countrywide) & NBP Head-office Group officials with certification of the proposed Solution.	50
Post Go-live Support Services Details • Local support cost for a resident engineer for 6 month Warranty period post go-live	To be given by the bidder

Note: Bidder is required to thoroughly examine the Section VII - Technical Requirement Document and may add any missing items in the above BOQ in relation to Section VII – Technical Requirements.

11. Delivery Schedule (DS) (Section-XI)

The bidder is advised to propose the Project Timelines in accordance with the Delivery Schedule mentioned below. The location of the project will be the NBP Head Office, Karachi, and the NBP DR Site.

Description	Delivery (calendar days) from the date of signing of the contract
Project Initiation Phase	Within 14 days
Hardware Arrangement, Installation	Within 60 days
Requirement Analysis Phase	Within 45 days
Designing and Development Phase	Within 120 days
System Integration Testing (SIT) Phase	Within 45 days
User Acceptance Testing (UAT) Phase	Within 30 days
Go-Live Phase	Within 30 days
Post Go Live Phase	Within 180 days

The bidder is required to provide a detailed implementation and delivery methodology, including a proposed timeline. This methodology should encompass all relevant information security tasks and milestones, ensuring the confidentiality, integrity, and availability of data throughout the project lifecycle. It is imperative that all procedures and processes align with the project management guidelines set forth by NBP. By adhering to these guidelines, the bidder will demonstrate a comprehensive understanding of the project's requirements and ensure structured and efficient execution that meets the bank's standards and expectations.

The bidder is advised to propose the Project Timelines in accordance with the Delivery Schedule mentioned below.

Description	Required Delivery from the date of signing of the contract	Location
Project Initiation Phase (Identifying Scope of Work)	Within 45 days	NBP Head Office, Karachi, and NBP DR Site
Project Implementation Phase (Requirement Analysis, Designing, Development/Customization, Implementation, Integration across all platforms, Data Migration (if required), Training and User Acceptance Testing, Security assessment, etc.) along with software, hardware, and their licenses as per the requirements mentioned in Annexure VII – Technical Requirements.	Within 6 Months	
Operational/Go-Live date of complete solution	Within 15 days after completion of the Project Implementation Phase	
Managed Services including but not limited to Support & Maintenance, including troubleshooting, technical Support, Bug Fixing, Release Upgrades, Software Patches, security assessment/vulnerabilities, a minimum of two cycles a year, etc.	Three Years after Go-Live Date as part of managed services. The Annual support & maintenance cost will be valid for the 4th and 5th years upon renewal from NBP.	

The bidder is required to provide a detailed implementation and delivery methodology, including a proposed timeline. This methodology should encompass all relevant information security tasks and milestones, ensuring the confidentiality, integrity, and availability of data throughout the project lifecycle. It is imperative that all procedures and processes align with the project management guidelines set forth by NBP. By adhering to these guidelines, the bidder will demonstrate a comprehensive understanding of the project's requirements and ensure structured and efficient execution that meets the bank's standards and expectations.

Bidder must provide on-site post-implementation support of Proposed Solution after Go-Live (completion of the entire scope).

12. Sample Forms (Section-XII)

Standard Bidding Documents (SBDs)

Table of Sample Forms

Note:
These are Sample forms only and may be used by bidders for submission in their proposals. For correct documentary evidence requirements, please refer to Section-VI Technical Requirements.

12.1 I-A. BID FORM

The Senior Vice President
Divisional Head (A)
Logistics Support Group
3rd Floor, NBP Head Office
I.I. Chundrigar Road
Karachi.

Dear Sir:

Having examined the bidding documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver the required item(s), goods, and services in conformity with the said bidding documents for the sum of *[total bid amount in words and figures]* or such other sums as may be ascertained Following the Schedule of Prices attached herewith and made part of this bid.

If our bid is accepted, we undertake to deliver the item(s), goods, and services Following the delivery schedule specified in the Schedule of Requirements.

If our bid is accepted, we will obtain the guarantee of a bank in a sum equivalent to five (05) percent of the Contract Price for the due performance of the Contract, in the form prescribed by NBP.

We agree to be bound by this bid for a minimum period valid for 270 days from the date fixed for bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We understand that you are not bound to accept the lowest or any bid you may receive.

Until a formal Contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award, shall be binding upon us, provided however, that you may cancel the tender at any time prior to the execution of a formal contract.

Dated this ______________ day of ______________ 20_____.

________________________________ ________________________________

[signature] *[in the capacity of]*

Duly authorized to sign bid for and on behalf of ________________________________

12.2 General Information Form

All partnership firms, sole proprietorships, companies, and each partner of a Joint Venture that is bidding must complete the information in this form. Nationality information should be provided for all owners or bidders that are partnerships or individually owned sole proprietorships.

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 owners*		
Name		Nationality
1.		
2.		
3.		
4.		
5.		
*	To be completed by all owners of partnerships or individually owned firms.	

12.3 General Solutions Experience Record

Name of Bidder or Partner of a Joint Venture

All individual firms and all partners of a Joint Venture must complete the information in this form with regard to the management of Solutions contracts generally. The information supplied should be the annual turnover of the bidder (or each member of a Joint Venture), in terms of the amounts billed to clients for each year for work in progress or completed, converted to PKR at the rate of exchange at the end of the period reported. The annual periods should be calendar years, with partial accounting for the year up to the date of submission of applications. This form may be included for Subcontractors only if the Bid Data Sheet for ITB clause 6.1 (a) explicitly permits the experience and resources of (certain) Subcontractors to contribute to the Bidder's qualifications.

A brief note on each contract should be appended, describing the nature of the Solution, duration and amount of contract, managerial arrangements, NBP, and other relevant details.
Use a separate sheet for each partner of a Joint Venture.

Bidders should not enclose testimonials, certificates, and publicity material with their applications; they will not be taken into account in the evaluation of qualifications.

Annual turnover data (applicable activities related activities only)

Year*	Turnover	PKR equivalent

* Commencing with the partial year up to the date of submission of bids

12.4 Joint Venture Summary (if any / if allowed)

Names of all partners of a Joint Venture

S. No	Name of the Partner(s)
1.	(Partner in charge)
2.	
3.	
4.	
5.	

The total value of annual construction turnover, in terms of Solutions billed to clients, in PKR equivalent, converted at the rate of exchange at the end of the period reported:

Annual turnover data (applicable activities only; PKR equivalent)

Partner(s)		Form 2	Year 1	Year 2	Year 3	Year 4	Year 5
1.	(Partner in charge)						
2.							
3.							
4.							
5.							
6.							
Totals							

12.5 Particular Solutions Experience Record

Name of Bidder or Partner of a Joint Venture

On separate pages, the bidder is requested to list contracts of a similar nature, and complexity, requiring similar information technology and methodologies to the contract or contracts for which these Bidding Documents are issued, and which the bidder has undertaken during the period, and of the number, specified in the BDS for ITB clause 6.1 (a). Each partner of a Joint Venture should separately provide details of its relevant contracts. The contract value should be based on the payment currencies of the contracts converted into PKR (Pakistani Rupees), at the date of substantial completion, or for ongoing contracts at the time of award.

12.6 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 contracts			
	Name of contract			
	Country			
2.	Name of Bank			
3.	Bank address			
4.	Nature of Solutions 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 the date of award for current contracts)			
	Currency			
7.	Equivalent amount PKR			
	Total contract: PKR _______;	Subcontract: PKR _______;	Partner share: PKR _______;	
8.	Date of award/completion			
9.	The contract was completed _____ months ahead/behind the original schedule (if behind, explain).			
10.	The contract was completed PKR _________ equivalent under/over the original contract amount (if over, provide an explanation).			
11.	Special contractual/technical requirements.			
12.	Indicate the approximate percentage of total contract value (and PKR amount) of the Solution undertaken by subcontract, if any, and the nature of such Solution.			

12.7 Financial Capabilities

Name of Bidder or Partner of a Joint Venture

Bidders, including each partner of a Joint Venture, shall provide financial information to demonstrate that they meet the requirements stated in the BDS for ITB clause 6.1 (a). Each bidder or partner of a Joint Venture shall complete this form. If necessary, separate sheets shall be used to provide complete banker information. A copy of the audited balance sheets shall be attached.

Autonomous subdivisions of parent conglomerate businesses shall submit financial information related only to the particular activities of the subdivision.

Name of banker			
Address of banker			
Telephone		Contact name and title	
Fax		Telex	

Summarize actual assets and liabilities in PKR (at the rates of exchange current at the end of each year) for the previous five calendar years. Based upon known commitments, summarize projected assets and liabilities in PKR equivalent for the next two calendar years, unless the withholding of such information by stock market-listed public companies can be substantiated by the bidder.

Financial information in PKR equivalent			Actual: Previous two years			
		5	4	3	2	1
1.	Total assets					
2.	Current Assets					
3.	Total Liabilities					
4.	Current Liabilities					
5.	Profits before taxes					
6.	Profits after Taxes					

Specify proposed sources of financing, such as liquid assets, unencumbered real assets, lines of credit, and other financial means, net of current commitments, available to meet the total construction cash flow demands of the subject contract or contracts as indicated in the BDS for ITB Clause 6.1 (a).

Source of financing		Amount (PKR equivalent)
1.		
2.		
3.		
4.		

Attach audited financial statements—including, as a minimum, profit, and loss account, balance sheet, and explanatory notes—for the period stated in the BDS for ITB clause 6.1 (a) (for the individual bidder or each partner of a Joint Venture). From SBP panel of Auditors maintained under section 35 (1) of banking companies' ordinance, 1962.

If audits are not required by the laws of bidders' countries of origin, partnerships, and firms owned by individuals may submit their balance sheets certified by a registered accountant and supported by copies of tax returns.

12.8 Personal Capabilities

Name of Bidder

For specific positions essential to contract management and implementation (and/or those specified in the Bidding Documents, if any), bidders should provide the names of at least two candidates qualified to meet the specified requirements stated for each position. The data on their experience should be supplied on separate sheets for each candidate.

Bidders may propose alternative management and implementation arrangements requiring different key personnel, whose experience records should be provided.

S. No	Title of Position Name of prime candidate	Name of alternate candidate
1.		
2.		
3.		
4.		
5.		

12.9 Candidate Summary

Name of Bidder

Candidate Information

Position		Candidate Prime	
		Candidate Alternate	
Name Of Candidate		Date Of Birth	
Professional Qualifications			
Present Employment		Name Of Employer	
Address of Employer			
Telephone		Contact (Manager/Personnel Officer)	
Fax		Telex	
Job Title of Candidate		Years With Present Employer	

Summarize professional experience over the last twenty years, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.

From	To	Company/Project/Position/Relevant technical and management experience

12.10 Technical Capabilities

Name of Bidder

The bidder shall provide adequate information to demonstrate clearly that it has the technical capability to meet the requirements for the Solution. In this form, the bidder should summarize important certifications, proprietary methodologies, and/or specialized technologies that the bidder proposes to utilize in the execution of the Contract Agreement and/ or related agreement.

12.11 Litigation History

Name of Bidder or Partner of a Joint Venture

Bidders, including each of the partners of a Joint Venture, shall provide information on any history of litigation or arbitration resulting from contracts executed in the last five years or currently under execution. A separate sheet should be used for each partner in a Joint Venture.

Year	Award For or Against Bidder	Name of Client, Cause of Litigation, & Matter in Dispute	Disputed Amount (Current Value, PKR Equivalent)

12.12 BID Security Form (Bank Guarantee).

[insert: Bank's Name, and Address of Issuing Branch or Office]

Beneficiary: [insert: Name and Address of NBP]

Date: [insert: date]

BID GUARANTEE No.: [insert: Bid Guarantee Number]

We have been informed that [insert: name of the Bidder] (hereinafter called "the Bidder") has submitted to you its bid dated [insert: bid date] (hereinafter called "the Bid") for the execution of [insert: name of contract] under Invitation for Bids No. [insert: IFB number] ("the IFB").

Furthermore, we understand that, according to your conditions, bids must be supported by a bid guarantee.

At the request of the Bidder, we [insert: name of Bank] hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of [insert: amount in figures] ([insert: amount in words]) upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

(a) has withdrawn its Bid during the period of bid validity specified by the Bidder in the IFB; or

(b) does not accept the correction of errors in accordance with the Instructions to Bidders (hereinafter "the ITB") of the IFB; or

(c) having been notified of the acceptance of its Bid by the NBP during the period of bid validity, (i) fails or refuses to execute the contract with you or (ii) fails or refuses to furnish the performance security, in accordance with the ITB.

This guarantee will expire: (a) if the Bidder is the successful bidder, upon our receipt of copies of the contract signed by the Bidder and the performance security issued to you upon the instruction of the Bidder; or (b) if the Bidder is not the successful bidder, upon expiry of ninety (90) calendar days after the expiration of the Bidder's bid.

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

____

[Signature(s)]

12.13 Supplier's Representative

Following GCC clause 1.1 (b) (IV), the Supplier's appointed Representative is:

Name: *[insert* ***name*** *or state* ***"to be nominated within fourteen (14) Days of the Effective Date"]***

Title: *[insert* ***title*** *or state* ***"to be specified within fourteen (14) Days of the Effective Date"]***

12.14 Performance Security Bank Guarantee

National Bank of Pakistan Beneficiary		Guarantee No.	
Executed on		Expiry Date:	
Name of Surety (Bank) and Address			
Name of Principal (Contractor) and Address			
Sum of Guarantee (expressed in words and figures)			
Contract No. And date			

Whereas, NBP ("NBP") has entered into a contract number [●] dated [●] ("Contract") with [●] (the "Contractor") for providing design, supply, installation, achieving operational acceptance of [*insert: a brief description of the Solution]* and services in respect thereof [●] to NBP.

And whereas, it is a condition of the Contract that the Contractor furnish a performance guarantee of a bank to NBP to secure the performance of the obligations of the Contractor under the Contract.

1) NOW THEREFORE, we, [●] waiving all objections and defenses, hereby irrevocably and independently guarantee to pay to NBP, without delay upon NBP's first written demand and without cavil or argument, any amount claimed by NBP up to the maximum amount of Rs [●] without requiring NBP to prove or to show grounds or reasons for such demand, up to the sum specified hereinabove, against NBP's written declaration that the Contractor has refused or failed to perform the aforementioned Contract. NBP may make any number of claims upon us up to the maximum amount secured hereunder and the guarantee shall stand reduced proportionately by the amount of the claims paid by us to NBP.

2) You shall not be obliged before making any demand upon us under this guarantee (a) to demand any payment of the Contractor (b) to take any legal proceedings against the Contractor, (c) to make any claim in winding-up of the Contractor, or (d) to exercise any right which you may have under any security or against any other surety for the obligations of the Contractor in respect of the Contract.

3) Our obligations under this guarantee shall not be discharged or effected by (a) any dissolution, winding-up, or corporate re-organization of the Contractor or (b) any transfer or extinguishing of any of the liabilities of the Contractor by any law, regulation, decree, judgment, order or similar instrument; or (c) on any other account, omission, or thing which but for this provision would or might constitute a legal or equitable discharge of a surety.

4) NBP may grant time and indulgence to the Contractor or vary the terms of the Contract, with or without notice to us, which notice is hereby waived, provided such time, indulgence, and variation does not increase the amount guaranteed.

5) The Contractor may by notice to us have the validity of this guarantee extended.

6) NBP shall be the sole and final judge for deciding whether the Contractor has duly performed its obligations under the Contract or has defaulted in fulfilling the said obligations and we shall pay without objection any amount claimed by NBP up to the sum named hereinabove upon demand from NBP forthwith or without any reference to the Contractor or any other person.

7) This guarantee shall remain valid up to [●] or up to the date that NBP issues a certificate to us stating that the Contractor has fulfilled all their obligations in a satisfactory manner, whichever date is later. We hereby waive the necessity of your demanding the said debt from the Contractor before presenting us with the demand.

8) Upon the expiry of the guarantee, we shall stand released and discharged of all obligations hereunder irrespective of whether the original guaranteed instrument is returned to us or not. This guarantee shall remain binding on our successors in interest.

____

Guarantor

Witnesses:

1. Signature	2. Signature
Name	Name
Title	Title

12.15 Advance Payment Bank Guarantee

Date: *[insert: date]*

IFB: *[insert: title and number of IFB]*

Contract: *[insert: name and number of Contract]*

To: *[insert: name and address of NBP]*

Dear Sir or Madam:

We refer to the Contract Agreement ("the Contract") signed on *[insert: date]* between you and *[insert:* name of Supplier] ("the Supplier") concerning design, supply, installation, achieving operational acceptance of [insert: a brief description of the Solution] and services in respect thereof.

Whereas, in accordance with the terms of the said Contract, NBP has agreed to pay or cause to be paid to the Supplier an advance payment in the amount of *[insert: amount in numbers and words, for each currency of the Advance Payment]* to the Supplier ("Advance Payment").

1. By this guarantee instrument we, the undersigned, *[insert: name of Bank]*, a bank organized under the laws of *[insert: country of Bank]* and having its registered/principal office at *[insert: address of Bank]*, (hereinafter, "the Bank") do hereby irrevocably guarantee payment of sums equal to the Advance Payment upon the first demand of NBP without cavil or argument and without reference to the Supplier, in the event that the Supplier fails to commence or fulfill its obligations under the terms of the said Contract. NBP shall be the sole judge of whether the Supplier has fulfilled its obligations or not.

2. You shall not be obliged before making any demand upon us under this guarantee (a) to demand any payment of the Supplier (b) to take any legal proceedings against the Supplier, (c) to make any claim in winding-up of the Supplier, or (d) to exercise any right which you may have under any security or against any other surety for the obligations of the Supplier in respect of the Contract.

3. Our obligations under this guarantee shall not be discharged or effected by (a) any dissolution, winding-up or corporate re-organization of the Supplier (b) any transfer or extinguishing of any of the liabilities of the Supplier by any law, regulation, decree, judgment, order, or similar instrument; or (c) on any other account, omission, or thing which but for this provision would or might constitute legal or equitable discharge of a surety.

4. You may grant time and indulgence to the Supplier or vary the terms of the Contract, with or without notice to us, which notice is hereby waived, provided such time, indulgence and variation does not increase the amount guaranteed.

5. This guarantee shall become operative from the date upon which the said Advance Payment is received by the Supplier and shall remain in force until the date upon which the Supplier has fully repaid the amount so advanced to NBP in accordance with the terms of the Contract and as evidenced by a certificate provided by NBP stating that the Supplier has fully repaid the Advance Payment. Upon issuance of the aforesaid certificate, this guarantee shall become null and void, whether the original is returned to us or not. Any claims to be made under this guarantee must be received by the Bank during its period of validity.

For and on behalf of the Bank

Signed:

Date:

in the capacity of: *[insert: title or other appropriate designation]*

Common Seal of the Bank

12.16 Integrity Pact

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

Contract Number: ________________ Dated: ______________

Contract Value: __________________

Contract Title: ___________________

________________________the [Bidder/Seller/Supplier/Contractor] hereby declares its intention not to obtain or induce 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, the [Seller/Supplier/Contractor] represents and warrants that it has fully declared the brokerage, commission, fees, 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 consultation fee or otherwise, with the object of obtaining or including 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 hereto.

The [Seller/Supplier/Contractor] 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, representation, or warranty.

The [Seller/Supplier/Contractor] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts, 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, the [Seller/Supplier/Contractor] 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 times the sum of any commission, gratification, bribe, finder's fee or kickback given by the [Seller/Supplier/Contractor] 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]

12.17 Declaration of Beneficial Ownership (where the value of the tender is above PKR 50 million)

Name	Father's Name / Spouse's Name	CNIC / NICOP / Passport Number	Nationality	Residential Address	Email Address	The date on which shareholding, control, or interest is acquired in the Business

In case of indirect shareholding, control, or interest being exercised through intermediary companies, entries, or other legal persons or legal arrangements in the chain of ownership or control, the following additional particulars are to be provided:

1	2	3	4	5	6	7	8	9	10
Name	Legal form (Company/Limited Liability Partnership/Association of Persons/Single Member Company/Partnership Firm/Trust/Any other individual, body corporate (to be specified)	Date of Incorporation/registration	Name of Registering Authority	Business Address	Country	Email Address	Percentage of Shareholding, control, or interest of BO in the legal person or legal arrangement	Percentage of Shareholding, control or interest of legal person or legal arrangement in the Company	Identity of the natural person who ultimately owns or controls the legal person or arrangement.

12.18 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: ....

12.19 Non-Disclosure Agreement (NDA)

This Non-Disclosure Agreement ("Agreement") is entered into by and between the undersigned bidder ("Bidder") and NBP ("NBP") in connection with the submission of a proposal for the "LOS Platform" as described in the Request for Proposal (RFP).

1. Definitions

1.1. "Confidential Information" shall mean all information, data, documents, specifications, plans, designs, proposals, or any other information disclosed by NBP to Bidder in connection with the RFP.

1.2. "Recipient" shall mean the party receiving Confidential Information, which, in this case, is the Bidder.

2. Business Scope

The Bidder acknowledges that the RFP contains sensitive and proprietary information related to NBP's requirements for the LOS Platform. The Bidder agrees to maintain the confidentiality of all such information and use it solely to submit a proposal for the RFP.

3. Representations and Warranties

3.1. The Bidder represents and warrants that it will not disclose or use any Confidential Information for any purpose other than the preparation and submission of the proposal for the RFP.

3.2. The Bidder further represents and warrants that its employees and agents who have access to Confidential Information will be bound by similar confidentiality obligations.

4. Disclosure of Information

4.1. The Bidder shall only disclose Confidential Information to individuals within its organization who have a legitimate need to know to prepare the proposal.

4.2. The Bidder shall take all reasonable measures to protect the Confidential Information from unauthorized disclosure, including but not limited to implementing physical, technical, and administrative safeguards.

5. Termination

5.1. This Agreement shall remain in effect until terminated in writing by either party.

5.2. Upon termination, the Bidder shall promptly return or destroy all Confidential Information in its possession, as directed by NBP.

6. Limitation of Liability

The Bidder understands and agrees that any unauthorized use or disclosure of Confidential Information may result in legal liability, including but not limited to damages and injunctive relief.

7. Remedies

In the event of a breach or threatened breach of this Agreement, NBP shall be entitled to seek injunctive relief, specific performance, and other equitable remedies in addition to any other legal remedies that may be available.

8. Dispute Resolution

Any dispute arising under or in connection with this Agreement shall be subject to resolution through arbitration in accordance with the laws of Pakistan. The prevailing party in such arbitration shall be entitled to recover its reasonable attorneys' fees and costs.

9. Signoff

This Agreement is binding upon the Bidder and NBP and their respective successors and assigns. By signing below, the Bidder acknowledges that it has read, understood, and agrees to be bound by the terms of this Non-Disclosure Agreement.

Bidder's Name: ________________________

Bidder's Authorized Signature: ________________________

Date: ________________________

National Bank of Pakistan Representative: ________________________

Date: ________________________

Please sign, date, and return a copy of this Agreement along with your proposal submission for the RFP. Non-Disclosure Agreement (NDA) on stamp paper.

12.20 Check List

Description	Documentary Proof/Attachments	
	Yes	No
Technical Requirements Matrix		
Bid Form without mentioning price details (in Technical Proposal)		
Bid Form with mentioning price details (in the financial proposal)		
Integrity Pact		
Any other Forms/Attachments as per RFP Requirements (Section – Sample Forms)		
All the attachments, proofs, and justifications as mentioned in the Technical Requirements of RFP (if any)		
Do not use the NBP logo.		
Company Letter Head or stamp & signatures		
Financial Envelope/Scanned		
Technical Envelope/Scanned		
No Calculation Error		
Other options should be quoted separately (other than RFP).		
AMC (4-5 Years) should be mentioned (if required) AMC period will be started after this post-implementation (including all MVPs/Iterations) Completion of scope.		

12.21 Bulk Man-days provision for Agile Software Maintenance & enhancement activities

- Provide Agile Software Project Management, Design, Development, and DevSecOps resources for API Gateway.
- Provide Agile Software Project Management, Design, Development, and DevSecOps resources for LOS.

12.22 Liability & Confidentiality

- NBP is not liable for any cost incurred by the Bidder in the preparation and production of a proposal (techno-functional) or for any work performed before the issuance of a contract or delivery.
- During this RFP process/system implementation phase, Bidder may acquire confidential information relating to NBP business, project, and/or customer, which the bidder agrees to always keep strictly confidential (even after the project has been completed) subjected to NDA sign-off. Note: If the bidder does not agree with the respective clauses, then they should explicitly state it within their proposal

12.23 Publicity

- The selected bidder is strictly prohibited from making any public announcements or media releases related to any aspect of the Request for Proposal (RFP) unless NBP explicitly grants written consent to the Bidder beforehand. This implies that the Bidder is bound to maintain complete confidentiality and refrain from disclosing any information or details pertaining to the RFP/project without prior authorization from NBP.

12.24 Project Plan & Work Breakdown Structure (WBS)

- Bidder must submit details on the project implementation methodology and resource assignment to each milestone of the implementation. High-level activities and work breakdown structure must be provided to furnish the proposed methodology and work plan in Man-Days for the whole project. "Pre-requisites" and "Resource Requirements" should be highlighted to accommodate expectations and planning.

12.25 Manuals/Documentation

Detailed documentation is to be maintained for implemented modules, including,

- Mapped business processes: This document outlines the existing business processes and how they will be supported by the software. It helps ensure that the software aligns with the organization's workflows and requirements.
- Product configurations: This document specifies the various configurations and settings within the software to tailor it to the organization's needs. It includes options related to features, user permissions, and other customizable elements.

- System configurations: Similar to product configurations, system configurations outline the settings and configurations at the system level. This may include server configurations, network settings, security configurations, and other system-level parameters.
- Data flow diagrams: Data flow diagrams illustrate how data moves through the software system, depicting inputs, processes, outputs, and data storage. They provide a visual representation of data flow and help identify potential bottlenecks or data integration points.
- Workflows: Workflows describe the sequence of steps and actions that users need to follow to complete specific tasks within the software. They provide a detailed overview of the user journey and interactions with the system.
- Business/Functional requirement documents: These documents capture the business needs and functional requirements of the software. They outline the desired features, capabilities, and expectations from a business perspective.
- System requirement documents: The system requirement documents specify the technical requirements and constraints for the software, including hardware, software, and network requirements. They help ensure that the system is designed and implemented to meet the necessary technical specifications.
- Technical design document: The technical design document provides an in-depth description of the software's architecture, components, modules, interfaces, and databases. It serves as a blueprint for the development and implementation team.
- Support and Troubleshooting Guides: Support and troubleshooting guides assist users and administrators in resolving common issues they may encounter while using the software. They provide instructions and solutions to address software problems effectively.
- Rollback steps and User Guide: The Software Rollback process entails systematically reverting to a prior software version to address issues. Accompanied by a User Guide, this guide provides clear, step-by-step instructions for users to navigate the rollback process efficiently. It outlines precautions, necessary actions, and potential challenges, ensuring a smooth transition back to a stable software state and minimizing disruptions.
- Disaster Recovery Plans: Disaster recovery plans outline procedures for recovering the software and data in the event of a catastrophic failure or other unforeseen circumstances. They help ensure business continuity and minimize downtime.

12.26 Training

Bidder is responsible for providing training that includes Functional and Technical training to NBP designated personnel and training material (User Manuals, System Management Manuals, Technical Manual, Training Manuals [should be in English] & Video Tutorials for all Business Segments Separately).

Training infrastructure, such as training rooms, projectors, etc., will be provided by NBP.

All costs and expenses incurred in training, which include traveling allowances (if required), daily allowances, and cost of training material, will be borne by the Bidder. The NBP shall not be liable for any costs and/or expenses concerning training and shall not entertain any requests/representations regarding bearing/sharing of costs and/or expenses.

The selected bidder will be expected to deliver to NBP one hard copy and one electronic copy of the documentation for each of the deliverables and the online context-sensitive help module included in the software to enable the NBP's personnel to use and understand the operations of the deliverables. The NBP may make additional copies of the Company-specific documentation for its internal use.

12.27 Installation/Commissioning

Installation and commissioning charges should be included in the Financial proposal, if any.

12.28 Bidder Information & Evaluation Questionnaire

Should have experience in having implemented the origination, monitoring, and workflow solution in at least two banks/FI in the local market.

Details of the Bidder			
1.	Name of the Bidder		
2.	Address of the Bidder		
3.	Constitution		
4.	Details of Incorporation of the Company	Date:	
		Reference No.	
5.	Valid Sales tax registration no. (for local companies only)		
6.	Name and designation of the contact person to whom all references shall be made regarding this RFP		
7.	Telephone No. (With Country Code)		
8.	E-Mail of the contact person		
9.	Zoom/Teams/Cisco Webex ID of the contact person		
10.	Website		
11.	How many employees does the Bidder have? (Pakistan Based & Internationally – mention separately)		
12.	Provide the Audit Reports of the last 03 consecutive Fiscal Years from SBP panel of Auditors maintained under section 35 (1) of banking companies' ordinance, 1962.		
13.	Details of geographical presence locally (in Pakistan) and in any other countries.		
14.	What are the criteria for requirements gathering?		
15.	Has your firm/organization ever been terminated for non-performance on a contract? If YES, describe in detail.		

16.	Please share levels of after-sales support, TATs, and structure.	

Nationality of Owners (To be completed by all owners of partnerships or individually owned firms.)		
Name		Nationality
1.		
2.		
3.		

Financial Details (as per audited Balance Sheets)				
1.	Year	2022	2023	2024
2.	Net worth (in PKR)			
3.	Turn Over (in PKR)			
4.	Profit after Tax (PAT) - (in PKR)			

Note:

NBP strictly prohibits any form of canvassing, lobbying, influence, or cartelization by any Bidder. Engaging in any such activities can lead to the disqualification of the Bidder.

Furthermore, the Bidder is required to respond to all the questions in the Request for Proposal (RFP) and provide comprehensive information as requested. Failure to provide essential information may lead to disqualification of the proposal. In other words, the Bidder must provide all the necessary information as specified in the RFP, failing which the proposal may be deemed incomplete and liable for disqualification.

The RFP shall have no interlineation or overwriting except as necessary to correct errors made by the bidder firm itself. Any such correction must be initiated by the person authorized to sign the RFP and stamped with the bidder's seal.

Required details must be properly filled out, and no bidder should be allowed alteration or modification once the RFP has been opened. NBP may seek and accept clarifications to the RFP that do not change the substance of the RFP. Any justification should be in writing.

12.29 Declaration for Clean Track Record

To,

The Divisional Head – Procurement Division

National Bank of Pakistan.
3rd Floor, Head Office Building, Karachi,
NBP Head Office,
Karachi.

Sir,

Having thoroughly reviewed the Terms & Conditions detailed in the RFP document associated with Bidder Selection for RFP No. RFP/2025-03/DBG/01, dated MM DD, YYYY, concerning the Request for Proposal for the Digital Transformation of the LOS Platform, I affirm that my company has not incurred any form of sanction or blacklist status from government, semi-government, or private entities in Pakistan or overseas. I hereby certify my capacity as a competent officer duly empowered by my company, to attest to this declaration.

We Remain,

Yours faithfully,

(Signature of the Bidder)

Printed Name

Designation:

Stamp

Date:

Business Address:

12.30 Contractual Terms & Conditions

- Proposals must be submitted on the company's letterhead, duly signed and stamped by authorized personnel. The NBP logo should not be printed on proposals.
- Proposals received after the specified submission date will be automatically disqualified.
- NBP reserves the right to accept or reject any or all proposals, in whole or in part, at its sole discretion, without assigning any reason.
- Proposals with incomplete or insufficient product/service details, or those that do not substantially conform to the requirements of this LOS-RFP, may be disqualified.
- All prices must be quoted exclusively in Pakistan Rupees (PKR) and must be inclusive of all applicable taxes, duties, and other charges. While all prices must be inclusive of taxes, bidders should be aware that tax rates are subject to change based on government directives. The quoted price shall remain fixed for the duration of the contract, and no price adjustments will be entertained by NBP due to changes in tax rates.
- Proposals must remain valid for a minimum of 120 days from the proposal submission deadline.
- All payments by NBP under any resulting contract will be made exclusively in Pakistan Rupees (PKR).
- The Performance Security will be discharged within thirty (30) days of NBP's issuance of a written Go-Live completion certificate for the entire scope of work upon receipt of a written request from the vendor. Submission of an incomplete or fraudulent Performance Guarantee will result in immediate disqualification and potential blacklisting of the bidder in accordance with Public Procurement Rules, 2004.

Bidders may be called to give a presentation of their solutions with their capabilities at their own cost, which will be considered for the techno-functional evaluation of the bidder.

If deemed necessary, NBP may seek the Proof of Concept (POC) of all available Standard Features (fully compliant) and Alternatives available against the required feature(s). Failure of the bidder to complete the demo as per the Standard Feature may result in the rejection/disqualification of the bid.

Bidders must, in all respects, observe and conform to the ‘Contractual Terms and Conditions’ set out in this RFP. NBP will shortlist bidders fulfilling eligibility criteria as detailed in this RFP. It is expressly understood that the determinations made by NBP in this regard shall be conclusive and legally binding.