REQUEST FOR PROPOSAL (RFP)

Evaluation of Service Providers providing Software Solutions for Public Financial Management System (PFMS)

JAMMU AND KASHMIR GRAMEEN BANK

RFP Ref. No:	Ref. No. JKGB/DAC/2026-27-3798
Issuing Department:	Digital And Alternate Channels (DAC)
Issue Date:	[10-Aug-2026]
Closing Date & Time:	[31-Aug-2026] @ 02:00 PM
Website:	www.jkgrameen.bank.in

Disclaimer

The information contained in this Request for Proposal (RFP) document or any information/documents provided subsequently to bidder(s), whether verbally or in documentary form by or on behalf of Jammu and Kashmir Grameen Bank (the Bank), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer and is only an invitation by the Bank to interested parties/Bidders for submission of bids. The purpose of this RFP is to provide the bidder(s) with information to assist in the formulation of their proposals. While effort has been made to include all information and requirements of the Bank, this RFP does not claim to include all the information each bidder may require. The Bank makes no representation or warranty and shall incur no liability under any law, statute, rules, or regulations as to the accuracy, reliability, or completeness of this RFP .The Bank may, in its absolute discretion, but without being under any obligation to do so, update, amend, supplement, or annul the information in this RFP.

1. Schedule for Request for Proposal (RFP) Process

S.No.	Activity / Description	Target Date / Timeline
1	Release of Request for Proposal (RFP)	[10-Aug-2026]
2	Last date for submission of written requests via email for clarifications	[18-Aug-2026] up to 04:00 PM
3	Last date and time for submission of sealed bids (Technical & Commercial)	[31-Aug-2026] up to 02:00 PM
4	Opening of Technical Bids	[31-Aug-2026] @ 03:00 PM
5	Address for communication/Submission of bids	DAC Cell, IT Department Jammu and Kashmir Grameen Bank, Head Office, Near Fruit Complex, Narwal, Jammu Pincode: 180006 JKGB e-Mail: dac.hoj@jkgb.bank.in/ anish.gupta@jkgb.bank.in Phone:9596608001/8809653333
6	Earnest Money Deposit	Rs. 2 Lac should be submitted online before last date of bid submission via NEFT **NEFT Details** IFSC Code: JAKA0GRAMEN Bank & Branch: Jammu and Kashmir Grameen Bank, Narwal, JAMMU, J&K- 180006 Account No. 2000070690000001 Account Name:- EARNEST MONEY DEPOSIT

**Note: The above dates are tentative. JKGB reserves the right to change the activity schedule and associated dates without prior notice. Quotations received after the stipulated closing date and time will not be considered.*

2. Introduction & Objective

Jammu and Kashmir Grameen Bank (JKGB), a Regional Rural Bank, was established by the amalgamation of J&K Grameen Bank and Ellaquai Dehati Bank by the Government of India Gazette Notification [S.O. 1628(E)] dated 7th April 2025.

The Bank operates with its Head Office at Narwal, Jammu (Pin-180006, Jammu & Kashmir).

Objective: The Bank invites sealed quotations from eligible, reputed vendors and solution providers with proven experience in the supply, design, and implementation of robust Software Solutions supporting Public Financial Management System (PFMS). The ultimate objective is to evaluate experienced market players capable of delivering a comprehensive, integrated solution to support growing transaction volumes and compliance frameworks.

3. Scope of Work

Account Validation & Beneficiary Onboarding

The solution shall provide real-time and bulk account validation services for beneficiaries, implementing agencies, PAOs, CDDOs and other entities as required by PFMS.

The system shall validate account number, IFSC, account status (active, dormant, frozen, closed), KYC compliance, beneficiary name verification, virtual account validation and beneficiary de-duplication.

The solution shall support processing of large-volume validation requests and provide configurable response reporting to PFMS.

Re-validation of failed accounts and maintenance of validation history shall also be supported.

Beneficiary & Agency Management

The solution shall support onboarding, modification, suspension, activation and deactivation of beneficiaries and implementing agencies.

It shall maintain beneficiary master data, agency hierarchies, scheme mappings and account mappings required by PFMS.

Complete audit trail and history management shall be maintained.

Payment Processing Framework

The solution shall support processing of DBT, Non-DBT, Treasury, PAO, CDDO, Zero Balance Account (ZBA), Hybrid TSA and other PFMS payment types.

The system shall support payment initiation, authorization, posting, settlement, return handling, reversal processing, retry processing and exception handling.

The solution shall support payment processing through CBS, NPCI and other external systems.

DSC and Certificate Based Processing

The application shall support digital signature certificate enrollment, validation and lifecycle management.

It shall verify signatures' digest values, certificate validity, signing limits and duplicate batch references.

The solution shall also support PFMS certificate-based signed files and provide approval workflows for certificate enrollment.

PFMS API-Based Integration Framework

The proposed solution shall support API-based integration with PFMS in compliance with the latest PFMS Office Memorandum and future integration guidelines.

The solution shall facilitate secure, real-time exchange of account validation requests, payment requests, transaction status updates, reconciliation data and reporting information through APIs.

The bidder shall provide API Gateway integration, API lifecycle management, authentication, authorization, monitoring and logging and version management capabilities.

During transition, the solution shall support both API-based and existing SFTP-based integration modes.

ISO 20022 Message Processing Frameworks

The solution shall support ISO 20022 messaging standards for payment initiation, payment status reporting, account reporting, reconciliation and settlement activities.

The system shall support validation, transformation, processing and generation of ISO 20022 compliant XML messages including pain, pacs and camt message formats.

The solution shall include message transformation and orchestration capabilities for seamless integration between PFMS, CBS, NPCI and other external systems.

Payment Acknowledgement, Response Logging & Status Management

The solution shall provide comprehensive acknowledgement management and response tracking capabilities for all payment, validation and reporting transactions exchanged between PFMS and the Bank.

The system shall capture, process and maintain complete audit trails of all acknowledgements and responses including REQACK, ACK, NACK, INIPAY, SUCCPAY, REJPAY, RETPAY, FAILPAY and any other status messages prescribed by PFMS.

The application shall maintain timestamp-wise transaction history and provide end-to-end traceability from payment initiation to final settlement or rejection.

The solution shall support response regeneration, message resend functionality, failed message reprocessing and reconciliation of all status messages exchanged between PFMS and the Bank.

Migration from SFTP-Based Integration to API & ISO 20022 Framework

The bidder shall be responsible for planning, designing, implementing, testing, and successfully migrating the existing SFTP/file-based PFMS integration framework to the new API-driven and ISO 20022 compliant architecture.

The migration approach shall include detailed gap analysis, impact assessment, API enablement, message mapping, parallel run support, reconciliation controls, rollback procedures, user acceptance testing, performance testing, and production cutover support.

The bidder shall ensure zero loss of transactions, complete auditability, data integrity, and seamless business continuity throughout the migration process and shall provide all necessary documentation, training, and post-go-live support for successful adoption of the new framework.

Transaction Lifecycle Tracking

The solution shall provide complete lifecycle tracking of every transaction including validation request, payment initiation, CBS posting, NPCI processing, beneficiary credit, return processing, reconciliation and final reporting.

The system shall support search and enquiry based on Account Number, Batch Reference Number, Transaction Reference Number, UTR Number and PFMS Reference Number.

Reconciliation & Settlement Management

The system shall perform automated reconciliation between PFMS, Middleware, CBS, NPCI, Treasury systems and external interfaces.

It shall support transaction-level, batch-level and settlement-level reconciliation. Exception management, mismatch reporting and integrity checks shall be provided.

NPCI Integration

The solution shall support integration with NPCI systems including APBS, ACH, NACH and future NPCI products.

It shall support file generation, encryption, decryption, acknowledgement processing, return processing, status reporting and reconciliation.

Treasury, PAO & CDDO Processing

The solution shall support maintenance of PAO and CDDO masters, treasury payment processing, payment authorization workflows, e-scroll generation, digital signing and reconciliation of treasury transactions.

FCRA Reporting Module

The solution shall support identification and maintenance of FCRA accounts, retrieval of account statements, generation of regulatory reports and certificate-based signing of reports for submission to PFMS and regulatory authorities.

NTRP Reporting Module

The solution shall support receipt and processing of transaction files from aggregator banks, settlement processing, reconciliation, e-scroll generation and reporting to PFMS.

Security, Audit & Compliance

The solution shall support LDAP/Active Directory integration, Role-Based Access Control (RBAC), Maker-Checker controls, encryption at rest and in transit, certificate management, HSM integration and comprehensive audit trails.

The solution shall comply with PFMS, RBI, NPCI, UIDAI and CERT-In guidelines.

Monitoring, Dashboard & MIS

The solution shall provide configurable dashboards, enquiry screens, operational reports, audit reports, exception reports and regulatory reports.

All reports shall be exportable in PDF, Excel, CSV and other standard formats.

The system shall support report scheduling, role-based access and ad-hoc query capabilities.

The solution shall provide, at a minimum, the following reports and dashboards:

Account Validation Reports

- Account Validation Status Report
- PFMS Valid Account Report
- Accounts Pending for Validation Report
- Invalid Account Validation Reason Report
- Account Wise Scheme Report
- Scheme Based Account Report

Branch & Agency Reports

- Bank Branch Details Report
- Branch Wise Payment Detail Report
- Transacting Agency Master Report
- Payment Topper Report (Volume, Value and Transaction Count)

Payment Processing Reports

- PPA Transaction Status Report
- E-Payment Files Received Report (PPA/DSC)
- Credit Transactions Pending Report
- Debit Transactions Pending Report
- Payment ACK Pending Report
- Payment Files Pending for Branch Maker Verification Report
- Payment Files Pending for Checker Approval Report
- Volume Report for PPA, DSC and Other PFMS Payment Types

Exception & Rejection Reports

- Doubtful Transaction Report
- Insufficient Funds Report
- Reject and Return Report
- Return Cases Reversed to Agency Report
- Initial Reject Report for NEFT Transactions
- Failed Payment Report
- Reprocessed Transaction Report

NPCI Reports

- NPCI Response Pending Report
- NPCI Summary Report
- APBS Transaction Status Report
- ACH Credit Outward Status Report
- NPCI Return and Reversal Report

User, Security & Audit Reports

- User Login Activity Report
- Role Permission Report
- User Access Audit Report
- Administrative Activity Report
- Transaction Audit Trail Report

Dashboard Requirements

Real-time operational dashboards covering:

- Account Validation Dashboard
- Payment Processing Dashboard
- API Monitoring Dashboard
- ACK/NACK Dashboard
- INIPAY/SUCCPAY/REJPAY Dashboard
- Reconciliation Dashboard
- NPCI Dashboard
- FCRA Dashboard
- NTRP Dashboard
- Exception Management Dashboard
- System Health & SLA Dashboard
- Volume Monitoring Dashboard

Ad-hoc Reporting

User-configurable reporting and enquiry capabilities based on:

- Account Number
- Scheme Code
- Agency Code
- Batch Reference Number
- Transaction Reference Number
- PFMS Reference Number
- UTR Number
- Date Range
- Payment Status
- Validation Status
- Branch Code
- User ID

Infrastructure, High Availability & Disaster Recovery

The bidder shall provide Production, UAT, Staging and Disaster Recovery environments.

The solution shall support High Availability architecture, database clustering, load balancing, backup and restoration, replication and disaster recovery mechanisms with defined RPO and RTO.

Testing Requirements

The bidder shall perform SIT, UAT, Volume Testing, Performance Testing, Security Testing, DR Testing and End-to-End PFMS Certification Testing. Detailed test reports and sign-offs shall be provided.

Operations & Support

The bidder shall provide implementation support, go-live support, 24x7 production support, L1/L2/L3 support, incident management, problem management, patch management, version upgrades and regulatory change support during the contract period.

Deliverables

The bidder shall provide HLD, LLD, Architecture Documents, API Specifications, Integration Documents, Installation Guides, Security Documents, Test Reports, User Manuals, Administrator Manuals, Training Material, Knowledge Transfer Documents, Go-Live Support Documentation and AMC Support Documentation.

Deployment Architecture & Infrastructure Scope

The proposed PFMS integration solution shall be hosted On-Premises within the Bank's Primary Data Center (DC) and Disaster Recovery (DR) site. The Bank will provision the baseline physical/virtual server hardware, operating systems, and core database licenses based on the bidder's sizing, and the successful bidder shall implement and fully operationalize the end-to-end solution on top of whatever minimal supported infrastructure the Bank provides. The bidder shall be fully responsible for supplying, deploying, configuring, hardening, and maintaining all required application software, middleware, API Gateways, ISO 20022 engines, and underlying runtime components across Production, UAT, Staging, and SIT environments. Furthermore, the bidder shall ensure high-availability (Active-Active/Active-Passive) clustering, support automated real-time replication with zero data loss for settled financial transactions and actively participate in bi-annual DR drills, perform VAPT vulnerability remediation, and guarantee that the delivered software architecture seamlessly scales for peak transaction growth for a minimum period of 5 years without additional software licensing or implementation costs to the Bank.

4. Eligibility Criteria

Bidders must fulfill all the following technical and corporate eligibility criteria to qualify for evaluation. Supporting documents as indicated must be enclosed with the Technical Offer (Envelope 1):

S.No.	Eligibility Criteria Requirement	Supporting Documents to be Submitted
1	The bidder must be registered with the Registrar of Companies/Firms in India and operational for at least three (3) years as on the date of this RFP.	Certificate of Incorporation / Registration issued by the competent Government authority.
2	The Bidder must possess a valid GST Registration and PAN number allotted by respective statutory authorities.	Copies of valid GST Registration Certificate and PAN Card.
3	The Bidder should have a minimum annual turnover of INR 03 Crores or more during the last three (3) financial years.	Copies of Audited Balance Sheets and/or Certificates from a Chartered Accountant (CA) for the preceding three (3) financial years. Enclose DIPP/MSE registration for relaxation.
4	The bidder must possess a positive net worth for the last 3 financial years and must be profitable for the FY 2025-26.	Audited Profit & Loss (P&L) Statements for the last 3 financial years along with the Auditor's Report/Certificate.
5	The Bidder must be an ISO/IEC 27001:2022 and ISO 9001:2015 certified company/firm, and must possess CMMI (Capability Maturity Model Integration) Level 3 or above certification.	Valid copies of ISO certificates and CMMI credentials clearly indicating the active validity period.
6	The Bidder must have designed, supplied, and successfully implemented a live PFMS Solution in at least 1 scheduled Commercial bank or RRB.	Credential letters or Copies of Purchase Orders from clients along with formal project Completion/Performance Certificates.
7	The Bidder must not be involved in any active Bankruptcy filings, insolvency	A formal, signed Undertaking to this effect executed by the authorized signatory.(Annexure

	petitions, or legal protection actions from creditors.	0)
8	The Bidder must not be blacklisted, debarred, or banned by any Central/State Government Department, PSU, Regulator, or Bank in India.	A formal, signed Undertaking on company letterhead to this effect.(Annexure 8)

5. Submission Guidelines & Proposal Format

5.1 Bid Security / Earnest Money Deposit (EMD)

5.1.1 The bidder should deposit a bid security / Earnest Money Deposit of Rs. 2,00,000/- (Rupees Two Lakh Only) through electronic means via NEFT, as mentioned in the bid details table. This must be valid for 180 days.

5.1.2 The EMD submitted by unsuccessful vendors will be released after the completion of the evaluation process with no interest earned. Unsuccessful bidders should submit the Letter for Refund of EMD/Bid Security as per **Annexure 5** to initiate the return.

5.1.3 The EMD of the successful bidder will be released without interest upon the bidder signing the Contract and furnishing the Performance Bank Guarantee as per the format mentioned in **Annexure 6**.

5.1.4 The Performance Bank Guarantee must be submitted within six months from the date of receipt of the purchase order or before the expiry of the EMD, for an amount equivalent to 10% of the project cost, valid for the entire contract period of 5 years. The Selected Bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project or during the contract period.

5.1.5 Forfeiture of Bid Security: The Bid Security will be forfeited in the following cases:

5.1.5.1 If a bidder withdraws its bid during the period of bid validity.

5.1.5.2 If a bidder makes any statement or encloses any form which turns out to be false/incorrect at any time prior to the signing of the Contract, or refuses to correct errors found in the bid.

5.1.5.3 If the Bank decides to conduct a reverse auction and any shortlisted bidder fails to participate in the reverse auction at least by way of a baseline entry.

5.1.5.4 In the case of a successful bidder, if the bidder fails:

- To execute the Contract within the stipulated time.
- To respond to the Purchase Order within the stipulated time.
- To furnish the Performance Bank Guarantee as outlined herein.

5.2 Performance Bank Guarantee

5.2.1 The Bank will require the selected bidder to provide a Performance Bank Guarantee as per the format mentioned in **Annexure 6**, within 180 days from the date of acceptance of the Purchase Order or signing of the contract (whichever is earlier), for a value equivalent to 10% of the Total Project Cost.

5.2.2 The Performance Guarantee must be valid for the contract period of 5 years. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project.

5.2.3 In case the selected bidder fails to submit the performance guarantee within the stipulated time, the Bank, at its discretion, may cancel the order placed on the selected bidder without giving any notice.

5.2.4 The Bank shall invoke the performance guarantee if the selected bidder fails to discharge their contractual obligations during the period, or if the Bank incurs any loss due to the bidder's negligence in carrying out the project implementation as per the agreed terms and conditions.

5.3 Language of Bid

5.3.1 The language of the bid response and all communications with the Bank must be in written English only.

5.3.2 Supporting documents provided with the RFP response can be in another language as long as they are accompanied by an attested translation in English. For the purpose of bid evaluation, the English translation will govern.

5.4 Period of Validity of Bids

5.4.1 Bids should remain valid for a period of at least 180 days from the last date prescribed by the Bank for bid submission.

5.4.2 In case the last date of bid submission is extended, the bidder shall ensure that the validity of the bid is calculated from the modified submission date. Any further extension of bid validity will be decided by the Bank as needed.

5.4.3 The price quoted in the Final Commercial Offer must remain valid for at least 180 days from the date of the offer.

5.5 Amendment of Bidding Documents

5.5.1 Prior to the deadline for bid submission, the Bank may, for any reason (whether at its own initiative or in response to clarifications sought by prospective bidders), modify the RFP contents/covenants by amendment.

5.5.2 Any such clarification or amendment will be notified exclusively on the Bank's website. No individual communication will be sent in this respect.

5.6 Submission Methodology & Envelope Structure

Bidders are required to submit their competitive proposals using a physical, two-part sealed envelope system. Both internal envelopes must be enclosed within a single outer Master Envelope as detailed below:

Envelope 1: Technical Offer

Super-scription: **"Technical Offer - Selection of Vendor for PFMS Solution for JKGB"**

Contents: This envelope must strictly contain internal technical documentation without any commercial references. It must include:

Annexure 1: Covering Letter on Company Letterhead, signed by the authorized signatory.

Annexure 2: Completed Eligibility Criteria compliance grid along with all verified supporting documents.

Annexure 3: Company Profile and past credentials.

Annexure B: Detailed Technical Proposal & Product Brochures aligned to the Scope of Work.

Note: *The EMD (NEFT details) must be kept inside this Original Technical Offer envelope.*

Envelope 2: Commercial Bid

Super-scription: "Commercial Bid - Selection of Vendor for PFMS Solution for JKGB"

Contents: This envelope must contain:

Annexure 4: Commercial Proposal Form, formatted exactly as per the prescribed template, duly signed and stamped by the authorized corporate signatory.

Envelope 3: Master Envelope

Super-scription: "Proposal for PFMS Software Solution for JKGB"

Contents: Both Envelope 1 and Envelope 2 must be placed inside this secure, sealed outer cover.

Labeling: The reverse side of all envelopes must explicitly state the Name, Business Address, and Primary Contact details of the bidding firm.

Submission Address

The complete, sealed Master Envelope must be submitted via registered post, courier, or delivered by hand to:

The General Manager IT,

Jammu and Kashmir Grameen Bank,

Head Office, Near Fruit Complex, Narwal, Jammu - 180006 (J&K).

5.7 No Commitment to Accept Lowest or Any Offer/Bid

5.7.1 The Bank shall be under no obligation to accept the lowest or any other offer received in response to this RFP and shall be entitled to reject any or all offers without assigning any reason whatsoever.

5.7.2 The Bank reserves the right to re-issue the tender/bid or make changes to the terms and conditions of purchase, which will be informed to all bidders.

5.7.3 The Bank will not be obliged to meet, have discussions with, or listen to representations from any bidder once their offer/bid is rejected. Any decision of the Bank in this regard shall be final, conclusive, and binding.

5.8 Bank's Right to Accept/Reject Any Bid and Cancellation of Tender Process

5.8.1 The Bank reserves the right to accept or reject in part or full any or all offers without assigning any reason thereof, even after the issuance of a Letter of Intent (LoI).

5.8.2 The Bank reserves the right to cancel the bidding process and reject all bids at any time prior to the contract award, without incurring any liability to the affected bidder(s) or any obligation to inform them of the grounds for the Bank's action.

5.8.3 If at any stage of the evaluation process it is discovered that a bidder does not meet the eligibility criteria or has submitted false/incorrect information, the bid will be summarily rejected and no further correspondence will be entertained.

5.8.4 The Bank reserves the right to amend, rescind, reissue, or cancel this RFP. The Bank is under no obligation to acquire any or all of the items proposed.

5.8.5 No contractual obligation whatsoever shall arise from this RFP process unless and until a formal contract is signed and executed by duly authorized officials of the Bank and the successful bidder.

6. Evaluation Methodology

6.1 Evaluation Process

6.1.1 The selection of bidders shall be based on the Quality cum Cost Based Selection (QCBS) Methodology, applying an aggregate weightage score of 30% for Technical Bids and 70% for Commercial Bids.

6.1.2 The percentage weights assigned to different modules during the Technical Bid evaluation are structured as follows:

#	Technical Evaluation Module	Weightage / Maximum Marks
1	Conformity to Technical Specifications (**Annexure 10**)	60 Marks
2	Solution Presentation / Live Demonstration	40 Marks
	Total Technical Marks	100 Marks

6.1.3 Financial/Commercial bids will only be opened for those bidders who obtain a minimum qualifying technical score of 70 marks out of 100.

6.1.4 The technical score shall be evaluated by the designated Technical Committee of the Bank using the following breakdown:

a) Technical Specifications (60 Marks): The aggregate score across all functional blocks mentioned in the technical specifications (Annexure-E). Marks will be distributed proportionally across these functional blocks based on their relevance and business importance.

b) Presentation/Demo (40 Marks): Evaluation of the live demonstration and presentation of the proposed software solution.

6.1.5 The Bank may, at its sole discretion, conduct a Reverse Auction. The reverse auction event will be managed by an e-procurement agency appointed by the Bank among the technically qualified bidders, allowing them an opportunity to bid dynamically.

6.2 Overall Evaluation Marks

6.2.1 The combined marks of both the Technical and Financial/Commercial proposals—calculated as per their respective weights—will determine the Final Attained Marks (F).

6.2.2 The formula utilized for calculating the final score to identify the successful bidder is as follows:

Final Marks (F) = (C-low / C) * 70 + (T / T-high)* 30

C-low: Lowest Price quoted, C: Bid Price as quoted by the bidder

T-high: Highest Technical Score Obtained, T: Technical Score obtained by the bidder

6.2.3 The bidder scoring the highest Final Marks (F) based on this formula shall be identified as the preferred vendor.

7. General Terms & Conditions

7.1 Key Operational Frameworks

7.1.1 Project Manager: The selected vendor shall assign an experienced Project Manager who will serve as the single point of contact (SPOC) for all operational activities. The Project Manager must possess delegated corporate authority to make immediate, on-site binding decisions regarding execution scope modifications.

7.1.2 Proposal Costs: The bidder shall entirely bear all costs associated with the compilation, preparation, and presentation submission of their proposal. Jammu and Kashmir Grameen Bank (JKGB) provides no explicit or implicit reimbursement for such upfront costs.

7.1.3 Engagement Term: The strategic engagement shall initially be structured for a fixed period of 5 years, subject to extension options based upon satisfactory operational performance metrics and mutual written consent.

7.1.4 Bidding Influence: Any documented effort by a bidding agency to influence the internal evaluation process, competitive comparison metrics, or final selection matrix will result in immediate disqualification and forfeiture of participation rights.

7.1.5 Confidentiality: The selected agency shall maintain strict confidentiality regarding all Bank-related content, customer data arrays, and strategies shared during the course of the project. No proprietary information may be shared with any third party without explicit prior written authorization from the Bank.

7.1.6 Arbitration & Jurisdiction: All disputes arising under this framework shall first be subject to amicable friendly consultation. Unresolved matters shall be referred to independent arbitration under the Arbitration and Conciliation Act, 1996. The seat of arbitration shall strictly be Jammu, and courts in Jammu alone shall possess exclusive jurisdiction.

8. Taxes and Duties

8.1 The Bidder shall solely be responsible for all payments (including any statutory payments) to its employees and shall ensure that at no time shall its employees, personnel, or agents hold themselves out as employees or agents of the Bank, nor seek to be treated as employees of the Bank for any purpose, including claims of entitlement to fringe benefits provided by the Bank, or for any kind of income or benefits.

8.2 The Bidder alone shall file all applicable tax returns for all of its personnel assigned hereunder in a manner consistent with its status as an independent contractor of services; and the Bidder will make all required payments and deposits of taxes in a timely manner.

8.3 The Bidder shall be liable to pay all applicable corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India.

8.4 Wherever the laws and regulations require deduction of such taxes at the source of payment, the Purchaser shall effect such deductions from the payment due to the Bidder. The remittance of amounts so deducted and issuance of certificates for such deductions shall be made by the Purchaser as per the laws and regulations in force.

8.5 Nothing in the Contract shall relieve the Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by the Bidder in respect of this Contract.

9. Rejection of Bid

The Bid is liable to be rejected if:

9.1 The document does not bear the signature and official stamp of the authorized person on each page.

9.2 The bid is incomplete, including the non-submission or non-furnishing of requisite documents, contains conditional clauses, or fails to conform to the terms and conditions stipulated in this Request for Proposal (RFP).

9.3 It is evasive or contains incorrect information.

9.4 Any form of canvassing, lobbying, external influence, or unauthorized querying regarding shortlisting status is attempted.

9.5 The bidder fails to comply with any of the points mentioned in the Scope of Work. Non-compliance with any point will lead to automatic rejection of the bid.

9.6 The bidder fails to submit the required RFP cost or Bid Security/EMD.

10. Modification and Withdrawals of Bid

10.1 No bid can be modified or withdrawn by the bidder subsequent to the final date and time specified for the submission of bids.

10.2 In the event of withdrawal of the bid by bidders after the deadline, the EMD will not be refunded by the Bank.

11. Warranty

11.1 All support and services necessary for provisioning, customization, deployment, maintenance, and smooth functioning of the PFMS PROJECT, as specified in this RFP, shall be considered part of the bundled deliverables under the contract period, whether under the initial warranty or during ATS/AMC.

11.2 The warranty shall be comprehensive and on-site (or as applicable under service model terms), starting from the date of Go-Live and shall remain valid for 1 year for software components. During the warranty, the bidder shall provide all corrective and preventive maintenance at no additional cost to the Bank.

11.3 Any corruption in the software, media, or associated services shall be rectified during the full period of the contract including warranty, if contracted, at no extra cost to the Bank.

11.4 The execution of the service(s) herein is and shall be strictly in accordance and in compliance with all Applicable Laws, as amended from time to time, the regulatory framework governing the same, and Good Industry Practice. The bidder must possess all permissions, consents, approvals, and licenses from all regulatory/statutory and non-regulatory authorities for executing the service(s).

11.5 The successful bidder warrants that Deliverables and the Services provided shall be as per the terms of this Agreement. The successful bidder must guarantee that the software supplied to the Bank is licensed, legally obtained, and fully complies with information/cyber security standards.

11.6 Software must be supplied with its original and complete printed documentation. The successful bidder shall be fully responsible for the warranty of all system components in respect of proper design, quality, material, and workmanship of the software and accessories covered by the offer.

12. Contract Period

12.1 The contract period for implementation of the required solution will initially be for a period of 5 years of support from the date of go-live/implementation. This includes 1 year of warranty and 4 years of Annual Technical Support (ATS) post-warranty.

12.2 If the Bank desires, the selected bidder must agree to provide Annual Technical Support for the application software for an additional 2 years after the expiry of the initial contract period on mutually agreed terms, renewable on a yearly basis. The Bank reserves the right to extend the contract for this further period of two years.

12.3 The successful bidder shall execute:

a) A Service Level Agreement (SLA), which incorporates all the services, terms, and conditions detailed herein and any other metrics prescribed by the Bank.

b) A Non-Disclosure Agreement (NDA).

12.4 The bidder shall execute the SLA and NDA within 1 month (or within the timeframe specified by the Bank) from the date of issuance of the purchase order. The contract must be executed by the authorized signatory of the bidder, backed by a submitted Power of Attorney.

12.5 The SLA will cover the performance and availability of the deployed solution. The Bidder shall bear entirely and exclusively all costs (in terms of time or finances) associated with the preparation and submission of its Bid. The Bank will in no case be held responsible or liable for these costs regardless of the conduct or outcome of the bid process, including cancellation, abandonment, or annulment.

13. AMC / ATS (Annual Maintenance Contract / Annual Technical Support)

13.1 After the expiry of the warranty period, the Bank will engage the selected bidder under an ATS/AMC framework for ongoing maintenance of the PFMS Project. The ATS shall cover software-level updates, new requirements issued by PFMS India, patching, audit requirements, security upgrades, and minor enhancements for a period of 4 years post-warranty.

13.2 ATS charges shall be payable as per the agreement terms, subject to successful delivery of performance reports, invoices, and compliance certificates.

13.3 The bidder must fully cooperate and provide tools, access, and resources for a seamless knowledge transfer or transition if so directed by the Bank.

13.4 The Bank reserves the right to terminate the ATS (if contracted) by giving the successful bidder a prior written notice of 1 month indicating its intention to terminate the Contract if the services rendered are found unsatisfactory. In that event, the vendor shall refund the proportionate amount of ATS collected for the remainder of that ATS period.

13.5 In the event that the above conditions are not met, the Bank reserves the right to outsource the software maintenance work to a third party or perform the same through its internal resources. In either scenario, the vendor shall provide the requisite maintenance training, technical know-how, and expert assistance to the persons or agencies authorized by the Bank at no extra cost.

13.6 Any decision in this regard by the Bank shall be final, conclusive, and binding on the selected Bidder.

14. Adherence to Cyber Security Policy

14.1 Bidders are liable for any failure to meet security standards or desired security aspects of all ICT resources as per the Bank's IT/Information Security/Cyber Security Policy. This policy framework will be shared with the successful bidder. Bidders must ensure robust Data Security and protection of all facilities and applications managed by them.

14.2 Deputed personnel must be thoroughly aware of the Bank’s IT/IS/Cyber Security Policy and maintain the utmost secrecy and confidentiality of the Bank’s data, including processes performed within Bank premises.

14.3 If at any time it comes to the notice of the Bank that data has been compromised, disclosed, misused, or misappropriated, the Bank will take suitable legal and administrative action as deemed fit. The selected vendor will be required to compensate the Bank to the fullest extent of the loss incurred.

14.4 The bidder must provide a formal undertaking promising not to disclose any Bank information, to maintain confidentiality as per policy, and to execute the Bank's "Non-Disclosure Agreement" document (Annexure 7).

14.5 Legal and regulatory requirements—including data protection, intellectual property rights, copyright, and relevant regulations for sub-contracting, along with the specific controls to be implemented—shall be integrated into the final supplier agreement.

14.6 All information resources (online or in-person) of the vendors and its partners shall be made accessible to the Reserve Bank of India (RBI) as and when sought.

14.7 Credentials of all vendor/third-party personnel accessing and managing the Bank's critical assets shall be systematically maintained in strict accordance with the Bank's policy.

14.8 The Bank shall evaluate, assess, approve, review, control, and monitor the risks and materiality of vendor/outsourcing activities. The bidder ensures full support for baseline system security configuration standards.

14.9 The Bank shall conduct effective due diligence, oversight, and management of third-party vendors, service providers, and partners. Criticality assessments will be performed regularly across all external arrangement layers.

15. Patent Rights

15.1 In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc., arising from the deployment or use of the systems procured via this RFP in India, the supplier shall act expeditiously to extinguish such claims.

15.2 If the Supplier fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be held liable for the compensation, including all associated expenses, court costs, and legal fees. The Bank will provide notice to the supplier of any such claim without delay.

16. Price Validity

16.1 Prices payable to the successful bidder as stated in the Contract shall remain firm and fixed. They are not subject to any changes under any circumstances during the contract period of 5 years.

16.2 The Total Cost should be exclusive of all applicable taxes and GST (SGST, CGST & IGST), which will be payable in actuals on the exact date of invoicing.

17. Authorized Signatory

17.1 The selected bidder shall explicitly indicate the authorized signatories permitted to discuss and correspond with the Bank regarding obligations under the contract.

17.2 At the time of signing the contract, the selected bidder shall submit a certified true copy of their Board Resolution, authenticated by the Company Secretary, authorizing specific official(s) to negotiate, sign agreements/contracts, raise invoices, accept payments, and handle formal correspondence. Proof of signature identification must be provided as required by the Bank.

18. Limitation of Liability

18.1 The Vendor’s aggregate liability for actual direct damages shall be limited to a maximum of the Contract Value, provided that this limit shall not apply to the following:

a) Infringement indemnities.

b) Bodily injury (including death) and damage to real property or tangible personal property caused by the Vendor's negligence.

c) Financial loss due to delays in service/delivery or claims for damages due to breach of contract.

d) Financial losses incurred by the Bank stemming from wrong coding, system breaches, bugs in customization/configuration, deployment/testing errors, or lapses in technical support.

18.2 For the purposes of this Section, “Contract Value” at any given point in time means the aggregate value of purchase orders placed by the Bank on the Vendor under this specific project.

19. Detailed Confidentiality Framework

19.1 The Vendor understands and agrees that all materials and information marked and identified by the Bank as 'Confidential' are valuable assets of the Bank and are proprietary. The Vendor will treat all confidential materials with the highest degree of care necessary to ensure unauthorized disclosure does not occur, and will not use or disclose any materials without prior written approval.

19.2 The Vendor shall not be liable for disclosure or use of information which is:

a) Possessed by the Vendor prior to receipt from the Bank, documented by written records.

b) Published or available to the general public through no fault or breach of confidentiality by the Vendor.

c) Obtained by the Vendor from a third party possessing a valid right to make such disclosure without confidentiality restrictions.

d) Developed independently by the Vendor without reliance on Bank resources.

19.3 If the Vendor is required by a judicial or administrative process to disclose confidential information, the vendor shall promptly notify the Bank to allow a reasonable time to oppose such process before any disclosure is made.

19.4 Any violation of this clause will cause the Bank irreparable harm where legal remedies alone are inadequate; the Bank is thus entitled to proper indemnification for quantified losses and may seek injunctive relief.

19.5 Nothing herein grants either party any right or license under copyrights, inventions, or patents owned by the other party. These confidentiality terms shall survive the expiration, termination, or cancellation of this tender.

19.6 Nothing contained in this contract shall limit the Vendor from providing similar services to third parties or reusing the skills, know-how, and experience gained by employees. The confidentiality obligations specifically survive for a period of 1 year post-termination/expiration of the Agreement.

20. Indemnity

20.1 The Company hereby indemnifies, protects, saves, and holds the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits, and other proceedings (including attorney fees) resulting directly or indirectly from:

i) Acts of omission or commission by the Company, its employees, agents, or sub-contractors.

ii) Breach of contractual terms, representations, warranties, or inaccurate covenants.

iii) Bona fide use of deliverables and services provided by the Company.

iv) Misappropriation of third-party trade secrets or infringement of patents, trademarks, or copyrights by provided components.

v) Claims made by employees or sub-contractor personnel deployed under this contract.

vi) Breach of confidentiality obligations.

vii) Gross negligence or gross misconduct solely attributable to the Company or its deployed agencies.

20.2 The Company shall indemnify the Bank against data loss, third-party intellectual property claims, and system malfunctions, provided that the Bank notifies the Company in writing immediately upon becoming aware of the claim, and grants the Company sole control of the defense and settlement negotiations.

20.3 Indemnity is limited to court or arbitration-awarded damages and excludes indirect, consequential, and incidental damages. However, it explicitly covers damages, losses, liabilities, or compensation suffered by the Bank arising out of claims made by its customers and/or regulatory authorities under frameworks like the Copyright Act, 1957 or Information Technology Act, 2000.

21. Intellectual Property Rights (IPR)

21.1 Each Party owns and retains all rights, title, and interests in its respective Pre-existing Intellectual Property and Independent Intellectual Property.

Independent Intellectual Property means any Intellectual Property developed by a Party independently of the applicable statement of work.

Pre-Existing Intellectual Property means any Intellectual Property owned by a Party or licensed to it prior to the commencement date of the work.

21.2 Title to all inventions and discoveries made jointly by the Parties resulting from work performed under this Agreement shall reside jointly between both Parties. The Parties shall mutually decide future courses of action regarding protection and commercial use of joint IPR in accordance with Indian Laws.

22. Non-Transferable Offer

This Request for Proposal (RFP) is strictly non-transferable. Only the specific bidder who has purchased and submitted the bid documents will be eligible for participation in the evaluation process.

23. Responsibility for Completeness

23.1 Any supplies and services not explicitly mentioned in this tender but necessary for the installation, configuration, testing, commissioning, performance, or overall completeness of the order shall be provided and made available by the vendor to ensure smooth operations under Indian banking conditions.

23.2 The bidder shall be held responsible for any discrepancies, errors, and omissions in the technical details submitted, irrespective of whether these details have been approved or reviewed by the Bank. The Bidder shall take all corrective measures immediately without extra cost to the Bank.

24. Ownership and Retention of Documents

24.1 All information processed, stored, or transmitted by the successful Bidder's application belongs exclusively to the Bank. By maintaining the application, the Bidder does not acquire implicit access or redistribution rights. Civil, criminal, or administrative penalties apply for failure to protect sensitive data appropriately.

24.2 Types of sensitive information covered include, but are not limited to: information subject to special statutory protection, legal actions, disciplinary items, complaints, IT security frameworks, pending cases, and civil/criminal investigations.

24.3 The successful Bidder shall not publish or disclose the details of any security safeguards designed, developed, or existing at any Bank location without prior written consent.

24.4 The Bidder must develop procedures to ensure that IT resources leaving the control of an assigned user (reassigned, removed for repair, replaced, or upgraded) are completely purged of all Bank data and sensitive application software.

25. Service Management

25.1 Service Level Framework

25.1.1 Effective support of in-scope services is a result of maintaining consistent service levels. This section lists the minimum service levels required to be maintained by the vendor, covering service availability, monitoring of in-scope services, and related components.

25.1.2 Operational Definitions:

Response Time: The interval from receipt of the first communication from the Bank to the Vendor (or the local contact person of the Vendor via any communication channel) informing them of a system malfunction, to the time a Vendor Engineer addresses the problem.

Restoration Time: The period from problem occurrence to the time the service returns to an operational status. This may include temporary workarounds or problem circumvention and does not necessarily include root cause removal.

Resolution Time: The period from problem occurrence to the time the root cause is entirely removed and a permanent fix is applied to prevent reoccurrence.

Down Time: The period when the system is unavailable due to a system issue. It represents the precise interval between reporting the failure and completing the repair (the sum of Response Time and Restoration Time).

25.2 Call Response, Resolution, and Uptime Commitments

The vendor must adhere to the following strict service windows and metric targets:

Service Metric	**Mandated Level**
Service Window	24x7
Response Time	Within 1 hour

Service Metric	**Mandated Level**
Resolution Time	Within 3 hours
Uptime Commitment	99.90%

25.2.1 Percentage Downtime Calculation: Percentage downtime refers to the aggregate downtime of the equipment during a quarter, expressed as a percentage of the total available time in that quarter i.e 90 * 24 hours

Example: If the aggregate downtime of the application is 2.16 hours (129 minutes and 36 seconds) during a 90-day quarter, the percentage downtime is calculated as:

* 100 / (90 * 24) = 0.10% (Considering days in quarter as 90)

25.2.2 Mean Time Between Failures (MTBF): The MTBF should be a minimum of 90 days, barring scheduled and mutually agreed-upon maintenance windows.

25.2.3 Downtime Exclusions: The following scenarios will be excluded from downtime computations:

- Downtime directly attributable to internal Bank issues.
- Scheduled downtime for routine maintenance activity, provided the successful bidder informs the Bank at least 1 week in advance (or 24 hours in advance for urgent situations).
- Downtime resulting from verified Force Majeure events.

25.3 Performance Impediments and Delays

25.3.1 If the vendor or its subcontractor(s) encounter conditions impeding the timely delivery of products or performance of services, the vendor shall promptly notify the Bank in writing of the delay, its likely duration, and its root causes.

25.3.2 Upon receipt of the notice, the Bank will evaluate the situation and may, at its sole discretion, extend the performance timeline with or without applying liquidated damages. Any such extension must be ratified via a formal contract amendment.

25.3.3 Except as explicitly provided above, any unauthorized delay by the vendor in fulfilling its delivery obligations shall render it liable to the imposition of liquidated damages.

26. Audit

26.1 Inspection Rights and Cooperation

26.1.1 The Bidder shall at all times, whenever required, furnish all information, records, and data stored in any form to internal, external, Bank-appointed, and statutory/RBI inspecting auditors, extending full cooperation.

26.1.2 The Bidder undertakes to cooperate with the Reserve Bank of India (RBI) to support its supervisory functions, furnishing all records or information called for during inspections.

26.1.3 The Bidder must facilitate these audits at no additional cost to the Bank, providing uninterrupted access to facilities and records, and must ensure the swift rectification of all identified irregularities within the designated timeframe.

26.1.4 The Bank retains the absolute right to audit the Application and its underlying Source Code using a qualified Security Auditor of its choice.

26.2 Compliance and Security Audits

26.2.1 The bidder shall ensure absolute compliance with the Bank's Information Security policy, mitigating any identified risks within the stipulated time without additional cost.

26.2.2 The selected bidder ensures that all Regulatory, Statutory, and Local Administration requirements are strictly adhered to across all deliverables over the entire contract period.

26.2.3 Periodic information security audits will monitor compliance with industry best practices. The frequency of these audits remains at the Bank's discretion. The scope of these audits includes, but is not limited to:

- Access and authorization procedures.
- Physical security controls.
- Input/output and Database (DB) controls.
- Backup and disaster recovery procedures.
- Network security controls and program change controls.

26.2.4 To safeguard data confidentiality, integrity, and availability, the Bidder shall grant the Bank's representatives physical and remote access to its installations, technical resources, operations, databases, documentation, and personnel.

26.2.5 The Bank has the right to audit manual or automated monitoring and performance measurement systems without prior approval or notice to the bidder.

27. Information Security

27.1 Data Protection and Asset Security

27.1.1 The Bidder and its personnel are strictly prohibited from carrying any written materials, layouts, diagrams, or digital storage media (hard disks, flash/pen drives, storage tapes, etc.) out of the Bank's premises without explicit written permission.

27.1.2 The Bidder’s personnel shall strictly follow the Bank's information security policy and all associated operational instructions.

27.1.3 The Bidder acknowledges that all business data and proprietary information shared or processed under this framework are highly confidential. The Bidder shall use a level of care to safeguard this data that is no less rigorous than the controls used to protect its own high-stakes proprietary information.

27.1.4 Access to the Bank's proprietary data shall be restricted exclusively to employees who require it to perform services under this Contract. The information shall not be used for any other purpose.

27.1.5 Upon termination of the Contract for any reason, or immediately upon demand by the Bank, the Bidder shall return all electronic and hardcopy information provided by the Bank, including all copies or reproductions, and securely delete residual instances.

27.2 Organizational Controls and Certifications

27.2.1 The Company certifies that it and its subsidiaries have implemented all necessary technical and organizational measures to protect the IT infrastructure and data used in business operations.

27.2.2 These controls must include robust oversight, access restriction layers, encryption protocols, physical safeguards, and comprehensive business continuity/disaster recovery plans designed to prevent unauthorized distribution, breach, destruction, or misuse.

27.2.3 The Company certifies that, to the best of its knowledge, there has been no security breach, compromise, or unauthorized access relating to any IT systems, networks, hardware, software, or data owned or maintained by the company or its third-party partners that would trigger a Material Adverse Effect.

27.2.4 The Company confirms it has not been notified of, and has no knowledge of, any underlying condition that could reasonably result in a material breach of its IT Systems and Data.

27.2.5 The Company shall maintain full compliance with all applicable privacy, security, data protection statutes, and the Bank's Supplier Security Policy.

27.2.6 The Bidder confirms that all IT assets, applications, and databases utilized are free from material bugs, errors, defects, Trojan horses, time bombs, malware, or other corruptants. (**Annexure 9**)

27.3 Safeguards, Audits, and Breach Notifications

27.3.1 The company is responsible for establishing an information security program designed to ensure the confidentiality of Customer Data and protect it against anticipated threats or operational hazards.

27.3.2 The Company will notify the Bank immediately of any security breach that impacts the Bank, its operations, or its corporate customers.

27.3.3 The Company shall maintain sufficient physical, technical, and administrative security safeguards to prevent unauthorized processing of Personal Data or the removal of Bank Confidential Information from its facilities. Written descriptions of these policies must be provided to the Bank upon request.

27.3.4 The Bank retains the right, upon reasonable written notice and during normal business hours, to conduct on-site security audits to verify compliance.

27.3.5 Annual Vendor Self-Audit: The Company shall perform, at its own expense, a comprehensive security audit at least once per year.

If the audit reveals issues that may adversely affect the Bank, the Company shall disclose the matter fully and provide a detailed remediation plan.

If no adverse matters are found, the vendor shall provide the Bank with a reasonable summary of the audit findings.

27.3.6 The Bank may utilize its internal staff or a third-party auditor to monitor the Company's security practices. If the Bank elects to run its own independent security audit, it will bear the cost, and the Company must promptly correct any deficiencies discovered.

27.3.7 Ad-hoc Bank Audits: Following a 30-day prior written notice, the Bank has the right to conduct a security audit during business hours (limited to once per year under standard conditions).

27.3.8 However, if the Bank has a good-faith belief that a material breach of security protections has occurred, the parties shall meet immediately. If the issue is not resolved within 30 days, an immediate audit shall be conducted and completed within 30 days thereafter at the Company's cost.

28. Force Majeure

28.1 Neither the Vendor nor the Bank shall be liable for penalties, liquidating damages, or termination for default if its delay or failure to perform obligations under the contract is the direct result of a Force Majeure event.

28.2 Definition: For purposes of this clause, "Force Majeure" means an event beyond the reasonable control of the affected party, not involving fault or negligence, and which is entirely unpredictable. Such events include wars, revolutions, epidemics, and severe natural disasters.

28.3 Notification: If a Force Majeure situation arises, the Vendor shall promptly notify the Bank in writing of the condition and its underlying cause. Unless otherwise directed by the Bank in writing, the Vendor shall continue to perform its contractual obligations as far as is reasonably practical.

29. Exit Clause

The Bank reserves the right to cancel the contract immediately upon the occurrence of one or more of the following conditions:

29.1 Failure of the successful bidder to accept the contract and furnish the required Performance Bank Guarantee (10% of the project cost) within 30 days from receipt of the purchase contract.

29.2 Material delays in delivery extending beyond the explicitly specified execution periods.

29.3 Delays in completing critical implementation, core customization, or final acceptance tests beyond the specified deadlines.

29.4 Serious functional discrepancies or persistent performance drops that disrupt the operational capabilities of the solution.

29.5 Any incident originating from the vendor's application or team resulting in direct financial or reputational loss to the Bank.

Note: In addition to contract cancellation, the Bank reserves the right to recover damages by encashing the Bid Security / Performance Guarantee. The Bank also retains the right to exit the contract at any point during its term by serving a 1-month notice period to the vendor.

30. Termination of Contract

30.1 Termination for Convenience or Non-Performance

30.1.1 The Bank reserves the right to terminate the contract if at any stage it determines that the performance of the vendor is unsatisfactory.

30.1.2 If termination occurs due to the failure of the successful bidder to perform its contractual obligations, the Bank shall have the right to invoke the Performance Bank Guarantee(s).

30.1.3 The Bank is entitled to terminate this Contract without incurring any cost, and recover all expenditure incurred, upon the happening of any of the following events:

30.1.3.1 The selected bidder commits a breach of any terms and conditions of the bid.

30.1.3.2 The successful bidder enters liquidation, bankruptcy, or receivership voluntarily or otherwise.

30.1.3.3 An attachment is levied or continues to be levied for a period of 7 days upon the effects of the Agreement.

30.1.3.4 The execution progress of the order is found unsatisfactory. In this scenario, the Bank reserves the right to have the remaining contract executed by another party of its choice by giving 1 month's notice. The selected bidder is bound to cover any additional expenditure incurred by the Bank.

30.1.3.5 Total deductions on account of accumulated liquidated damages exceed 10% of the total contract value.

30.1.3.6 Persistent non-satisfactory performance during active implementation or post-go-live operations.

30.1.3.7 Acts of omission or commission by the bidder, its employees, its agents, or members of its consortium during performance of service.

30.1.3.8 Failure to integrate or implement the project as per the mandatory requirements specified in this RFP.

30.1.3.9 Material discrepancies in the Deliverables and Services. The Bank reserves the right to source alternative solutions at the risk, cost, and responsibility of the selected bidder.

30.1.3.10 The selected bidder is found to be indulging in fraudulent practices.

30.1.3.11 The Bank suffers a clear loss of reputation due to the activities or conduct of the successful bidder.

30.1.3.12 The vendor attempts to subcontract or assign the contract contrary to the agreed terms without obtaining prior written permission from the Bank.

31. Migration

31.1 In the event of termination or expiry of the contract term, the Vendor must fully cooperate with the Bank to seamlessly migrate all PFMS data and other critical information as required by the Bank at no extra cost.

31.2 Upon successful completion of data migration and verification by the Bank, the Vendor shall securely delete all data belonging to the Bank that exists within the Vendor's systems or environments.

32. Arbitration, Governing Laws, and Dispute Resolution

32.1 Dispute Resolution Process

32.1.1 Any dispute arising out of or in connection with this agreement shall first be resolved through friendly internal negotiations between parties.

32.1.2 If the dispute cannot be settled amicably within fourteen (14) days, the matter shall be submitted to binding arbitration under the Arbitration and Conciliation Act, 1996 through a sole arbitrator appointed by mutual consent.

32.1.3 The seat and place of arbitration shall strictly be Jammu, India. The language of the arbitration proceedings, documentation, and formal communications shall be English.

32.1.4 The decision of the sole arbitrator shall be final, conclusive, and binding upon both parties. The fees and expenses of the arbitrator shall be borne equally by each party.

32.2 Governing Laws

32.2.1 The Contract, its core meaning, interpretation, and the relationship between the parties shall be governed entirely by the applicable laws of the Union of India, read alongside the local laws of Jammu & Kashmir.

32.2.2 The Vendor agrees to submit exclusively to the jurisdiction of the courts under which the Registered Head Office of the Bank falls (Jammu).

Annexure 1: Technical Bid Covering Letter

(To be provided on the Bidder's Company Letter head)

Date: [_________________]

To,
The General Manager IT,
Jammu and Kashmir Grameen Bank,
Head Office, Narwal, Jammu - 180006.

Sub: Submission of Response to RFP for Implementation of PFMS Software Solution

Madam / Sir,

Having examined the complete RFP document, including all scope definitions, terms, conditions, and annexures, the receipt of which is hereby formally acknowledged, we, the undersigned, offer to supply, implement, and maintain the PFMS Software Solution in strict conformity with the deliverables outlined.

We hereby declare and confirm that:

- (i) We agree to abide by this Proposal and its associated financial elements for a fixed period of 180 days from the opening date of the commercial bid, and it shall remain binding and subject to acceptance at any point prior to the expiry of this window.
- (ii) Our Company/Firm/Agency currently possesses an unblemished corporate record. We are not declared ineligible, nor have we been formally blacklisted, barred, or structurally penalized for corrupt, fraudulent, or unsatisfactory practices by any State/Central Government Department, Regulator, Bank, or Public Sector Undertaking in India.
- (iii) We understand that if any statement or compliance declaration made in our bid package is discovered to be false, incorrect, or intentionally misleading, JKGB reserves the absolute right to cancel our bid, terminate any resultant contracts, and initiate formal debarment procedures.

Yours faithfully,

____

Authorized Signatory Signature
Name: ______________________________
Designation: _________________________
Company Seal:

Full Corporate Address: ____
Telephone / Mobile No: ________________ Email ID: _______________________

Annexure 2: Eligibility Criteria Compliance Matrix

Bidders must fill this matrix completely and append the exact supporting documentation indicated.

S.No.	Eligibility Criteria	Document Attached (Brief Description) / Compliance
1	Company/Firm Registration (>= 3 Years)	
2	Valid PAN & GST Registration	
3	Annual Turnover Criteria (>= 03 Cr)	
4	Positive Net Worth & Profitability (Last 3 FYs)	
5	ISO 27001:2022, ISO 9001:2015 & CMMI Lvl 3	
6	PFMS Solution Proof in at least 1 Scheduled commercial bank/RRB	
7	Non-Bankruptcy Undertaking enclosed	
8	Non-Blacklisting Undertaking enclosed	

Authorized Signature: ________________________
Name & Designation: _________________________
Date: _____________________ Place: __________
Company Stamp:

Annexure 3: Company / Agency Profile Template

Information Sought	Bidder Response / Details
Registered Business Name	
Legal Constitution (Proprietorship / Partnership / LLP / Private Ltd / Public Ltd)	
Registered Office Address	
Corporate Website URL & Main Email Address	
GST Registration Number (Enclose Certificate copy)	
Income Tax PAN / TAN (Enclose Copy)	
Name of Designated Authorized Signatory	
Designation of Authorized Representative	
Primary Contact Number & Hand phone No.	

Annexure 4: Commercial Bid Format

(To be enclosed strictly within a separate sealed Envelope 2)

Bidders must itemize all components required to deliver the core functional requirements detailed under the Scope of Work.
All prices must be quoted in Indian Rupees (INR) and exclusive of applicable GST elements.

S.No.	Component / Deliverable Item	Base Unit Cost (INR)	Total Price (INR)
1	Core PFMS Software Application License Fee (Enterprise/Bank-wide)		
2	Implementation, Customization & CBS Integration Charges (Finacle APIs)		
3	Aadhaar Vault & NPCI System Pipeline Integration Fee		
4	Annual Maintenance Contract (AMC) / Support Charges for 4 Years(2^{nd} year onwards)		
5	Total Commercial Bid Value (L1 Evaluation Basis)		

Total Commercial Quote in Words:
____

We certify that the costs quoted above are comprehensive, turn-key in nature, and cover all infrastructure dependencies, functional requirements, and ongoing support parameters mentioned in this RFP without any hidden exclusions.

Authorized Signature: _______________________
Name & Designation: _________________________
Company Stamp:

Annexure 5 - Letter for Refund of EMD

LETTER FOR REFUND OF EMD
(To be submitted by the unsuccessful bidders)

Date:

General Manager IT,
Head Office, Jammu and Kashmir Grameen Bank.,
Narwal, Jammu

We ___________ (Company Name) had participated in the RFP PFMS Solution as Service and we are an unsuccessful bidder.

Kindly refund the EMD submitted for participation. Details of EMD submitted are as follows

NEFT DETAILS:
DATE:
REFERENCE ID/TRANSACTION ID:
AMOUNT:

Bank details to which the money needs to be credited via NEFT are as follows

1. Name of the Bank with Branch
2. Account Type
3. Account Title
4. Account Number
5. IFSC Code

Sign

Name of the signatory:

Designation:

Company Seal

Annexure 6 – Format of Performance Bank Guarantee

(FORMAT OF PERFORMANCE BANK GUARANTEE)

Bank Guarantee No: …………………………..

Dated: …………………………………..

Bank: ………………………

To

General Manager IT,

Jammu and Kashmir Grameen Bank Head office,

Narwal

Jammu-180 006 (India)

WHEREAS_____________ (Company Name) registered under the Indian Companies Act 1956 and having its Registered office at_____________, hereinafter referred to as the BIDDER has undertaken project for PFMS Solution on need basis of Jammu and Kashmir Grameen Bank in terms of the Purchase Order bearing No.____________________ dated__________, hereinafter referred to as "the CONTRACT.

AND WHEREAS in terms of the Conditions stipulated in the said Contract, the BIDDER is required to furnish, performance Bank Guarantee issued by a Scheduled Commercial Bank in your favor to secure due and satisfactory compliance of the obligations of the BIDDER in accordance with the Contract;

THEREFORE, WE,……………………………… (Name of the Bank) furnish you this Performance Guarantee in the manner hereinafter contained and agree with you as follows:

1. We,……………………………………… Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on a demand, which has to be served on us before the expiry of this guarantee, time being essence of the contract, from you stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by you by reason of breach by the said Bidder of any of the terms and conditions contained in the Contract or by reason of the Bidder's failure to perform the said contract. Any such demand made on us within the time stipulated above shall be conclusive as regards the amount due and payable by us under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding___________(Rupees______________________________Only).

2. We undertake to pay to you any money so demanded notwithstanding any dispute/s raised by the Bidder in any suit or proceeding before any Court or Tribunal relating thereto, our liability under these presents being absolute and unequivocal. The payment so made by us under this guarantee shall be a valid discharge of our liability for payment there under and the Bidder shall have no claim against us for making such payment.

3. We further agree that, if demand. as stated above, is made on us within the stipulated period, the guarantee herein contained shall remain in full force and effect and that it shall continue to be enforceable till all your dues under or by virtue of the said contract have been fully paid and your claims satisfied or

discharged or till you certify that the terms and conditions of the said contract have been fully and properly carried out by the said Bidder and accordingly discharge this guarantee. Provided, however, serving of a written claim / demand in terms hereof on us for payment under this guarantee on or before the stipulated period, time being the essence of contract, shall be a condition precedent for accrual of our liability / your rights under this guarantee.

4. We further agree with you that you shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder, to vary any of the terms and conditions of the said Contract or to extend time for performance by the said Bidder from time to time or to postpone for any time or from time to time any of the powers exercisable by us against the said BIDDER and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of such variation, or extension being granted to the said Bidder or for any forbearance, act or omission on our part or any indulgence by us to the said Bidder or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. This Guarantee will not be discharged due to the change in the constitution of our Bank or the Bidder.

6. We further agree and undertake unconditionally to pay you the amount demanded by you in writing irrespective of any dispute or controversy between you and the BIDDER.

7. We lastly undertake not to revoke this guarantee during its currency except with your written Consent.

NOTWITHSTANDING anything contained herein above;

(i) Our liability under this Guarantee shall not exceed `...(Rupees... only) ;

(ii) This Guarantee shall be valid up to and including the..................................(mention date); and

(iii) We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before the expiry of this guarantee.

Dated the ………………… day of ………… 20 ……. For BANK

Authorized Signatory

Annexure 7 – Confidentiality / Non-Disclosure Agreement

This CONFIDENTIALITY AGREEMENT (the "Agreement") entered into on this _ day of 202__, and shall be deemed to have become in full force and effect from (the "Effective Date").

BY and between M/s.________________ a company incorporated under the provisions of the Companies Act, ________ in force in India, having its registered office at ____ (hereinafter referred to as "--------" or "Vendor" which expression shall, unless it be repugnant or contrary to the context or meaning thereof, mean and include its, successors and permitted assigns) of the ONE PART AND

Jammu and Kashmir Grameen Bank, established on 01st May 2025 through amalgamation of J&K Grameen Bank and Ellaquai Dehati Bank vide Government of India gazette notification CG-DL-E-07042025-262329 dated 07 April 2025. (hereinafter referred to as "Jammu and Kashmir Grameen Bank" or "Bank" which expression shall, unless it be repugnant to the context or meaning thereof, mean and include its successors and permitted assigns), of the OTHER PART:

---------- and the Bank shall hereinafter jointly be referred to as "Parties" and individually as a "Party".

In this Agreement, "Affiliate" means any entity which from time to time Controls, is Controlled by or is under common Control with the relevant party or entity, where "Control" means having the ability (including, without limitation, by means of a majority of voting rights or the right to appoint or remove a majority of the board of directors) to control the management and policies of an entity.

W H E R E A S: -

i. Vendor inter-alia is engaged in the business of providing IT related solutions & services to various business entities in India & abroad.

ii. Jammu and Kashmir Grameen Bank has agreed to disclose, transmit, receive, and/or exchange certain "confidential information" to cover the business transaction between parties for the provision of services related to " ("the Purpose") as more particularly described in Purchase Order no , issued by Jammu and Kashmir Grameen Bank in favor of M/s. ----------------------.

NOW THIS AGREEMENT WITNESS:

1. Interpretation

In this Agreement "Confidential Information" means all information belonging to a Party that is or has been disclosed to one Party (the "Receiving Party") by the other Party (the "Disclosing Party") in connection with the business transacted/ to be transacted between the Parties. Confidential information shall also include any copy, abstract, extract, sample, note or module thereof. The Receiving Party may use the Confidential Information solely for and in connection with the business transacted/ to be transacted between the Parties.

Notwithstanding the foregoing, "Confidential Information" shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes or is in possession of the Receiving Party, legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any obligation of confidentiality prior to receiving it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or (e) is disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

2. Confidentiality:

2.1 Except to the extent as agreed herein, the Receiving Party agrees to regard, preserve and keep as secret and confidential all Confidential Information of the Disclosing Party or its clients or any member of their group disclosed under this Agreement. In maintaining confidentiality hereunder the Receiving Party agrees and accepts that it shall not, either on its own account or jointly with or for any other person, firm, company or any other entity, without obtaining the written consent of the disclosing party.

I. disclose, transmit, reproduce or make available any such Confidential Information to any person firm, company or any other entity other than its directors, partners, advisers, agents or employees, who need to know the same for the purpose of evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose aforesaid; or

II. use the Confidential Information for any purpose other than evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose for which it is disclosed; or

III. disclose, announce or otherwise publicize the existence of its association with the Disclosing Party or the existence of the project with the Disclosing Party or any other arrangement (existing or possible) between the disclosing party, its clients or itself in connection with any project/assignment; or

IV. use any such Confidential Information for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its clients or any member of their group or their projects.

2.2 The Receiving Party also agrees and accepts that it may endeavor:

I. use at least the same degree of care in safeguarding such Confidential Information as it uses for its own Confidential information of like importance and such degree of care shall be at least that which is reasonably calculated to prevent such inadvertent disclosure;

II. keep the Confidential Information and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;

III. limit access to such Confidential Information to those of its (including its Affiliates‟) directors, partners, advisers, agents or employees who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees so involved to protect the Confidential Information in the manner prescribed in this Agreement; and

IV. upon discovery of any disclosure or suspected disclosure of Confidential Information, to take reasonable effort to as per the circumstances, to inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information, in whatsoever form, including any and all copies thereof.

3. Return or destruction:

The Receiving Party may, upon completion of the purpose mentioned aforesaid or at any time on receipt of a written demand from the disclosing party: i) immediately return all written Confidential Information and all copies thereof provided to, or produced by, it or its advisers, as the case may be, which is in such party's possession or under its custody and control; ii) to the extent practicable, but without prejudice to the obligations of confidentiality herein, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the other party; iii) so far as it is practicable to do so (but, in any event, without prejudice to the obligations of confidentiality contained in this Agreement), immediately expunge any Confidential Information relating to the Disclosing Party or its clients or any member of their group or their projects from any computer, word processor or other device in its possession or under its custody and control.

4. Permitted disclosure:

The provisions of paragraph 2 shall not restrict any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, official or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the other party of such requirement with a view to providing the opportunity for the Provider to contest such disclosure or otherwise to agree the timing and content of such disclosure.

5. Ownership of Information:

Except to the extent as agreed herein, the Confidential Information and copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party or its clients and its disclosure shall not confer on the Receiving Party any rights (including any intellectual property rights) over the Confidential Information whatsoever beyond those contained in this Agreement.

6. No Representation:

Neither the disclosure, transmission receipt or exchange of Confidential Information nor anything else in this Agreement will constitute an offer by or on behalf of the Disclosing Party or be construed as soliciting any business or organization changes or any assurance of any business commitment or an inducement to incur / undertake any obligations not specified herein and neither party will be under any obligation to accept any offer or proposal which may be made by the other or on behalf of such other party.

7. Remedies and Relief:

The parties hereto acknowledge that remedies at law may be inadequate to protect the

Disclosing Party or its clients against any actual breach of this Agreement by the Receiving Party, and, without prejudice to any other right and remedies otherwise available to the Disclosing Party or its clients, the Receiving Party agrees that Disclosing Party has a right to seek injunctive relief in its favor upon proof of actual damage and upon establishment of the fact that such actual damage has taken place due to reasons directly attributable upon the Receiving Party. Such injunctive relief shall be in addition to any other remedies available hereunder, whether at law or equity. Disclosing Party shall be entitled to recover its cost and fees, including Advocate's fees, incurred in obtaining any such relief. Further, in the event of litigation relating to this Agreement, the prevailing party shall be entitled to recover its cost and expenses including Advocate's fees.

8. No Assignment

This Agreement shall not be assigned by either party, by operation of law or otherwise, without the prior written consent of the other party. This Agreement shall inure to the benefit of and will be binding upon the parties‟ respective successors and permitted assigns.

9. Severability
In the event that any of the provisions contained in this Agreement is found to be invalid, illegal or unenforceable in any respect by a Court of competent jurisdiction, the validity, legality, or enforceability of the remaining provisions contained in this agreement will not be in any way affected or impaired by such a finding.

10. Delay or Waiver

No delay or failure of either Party in exercising any right hereunder and no partial or single exercise thereof shall be deemed of itself to constitute a waiver or an expectation of non-enforcement of such right or any other rights hereunder. No waiver of any provision of this Agreement shall be valid unless the same is in writing and signed by the party against whom such waiver is sought to be enforced. A waiver or consent given by either party on any one occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.

11. Notices

Notices as required by this Agreement shall be sent to the Parties at the addresses mentioned first herein above or such other addresses as the Parties may designate from time to time, and shall be sent by certified or registered mail with acknowledgement due on receipt.

12. Term

This Agreement shall commence from the Effective Date of this Agreement and shall be valid for a period of --- ------------ years there from. Confidentiality obligations under this Agreement shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain, without breach of the agreement. Either Party may terminate this Agreement for breach, if the defaulting Party fails to rectify the breach within the one-month notice period issued by the no defaulting Party. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease any and all disclosures or uses of Confidential

Information; and at the request of Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

13. Governing Law

The provisions of this Agreement shall be governed by the laws of India and shall be subject to the exclusive jurisdiction of courts in Jammu.

14. Indemnity

The Receiving Party agree to indemnify and hold harmless the Disclosures against all costs, liability, losses and claims incurred by the Disclosing Party as a result of a breach of this Agreement.

15. Modification

Modification to any of the provisions of this Agreement shall be void unless it is writing and duly executed by Parties.

16. Headings

The headings given herein above are for ease of reference only and shall not attach or have any effect/ meaning whatsoever contrary to what is stated in the agreement.

17. Counterparts

This Agreement has been signed in duplicate, each of which shall be deemed to be an original. The exchange of a fully executed Agreement (in counterparts or otherwise) by fax shall be sufficient to bind the parties to the terms and conditions of this Agreement.

IN WITNESS WHEREOF THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED BY THEIR AUTHORIZED REPRESENTATIVES ON THIS ______ DAY OF ____ _____ 2026_

Signed and delivered by	Signed and delivered by
M/s ________________________	Jammu and Kashmir Grameen Bank
Signed by:	Signed by:
Name ……………….…………….	Name ……………….……………….
Title ………………………………. in the presence of	Title ………………….…………….. in the presence of
…………………..…………………..…..	…………………..…………………….

Annexure 8 - Undertaking by Bidder

Place:

Date:

To
General Manager IT,
Head Office, Jammu and Kashmir Grameen Bank.,
Narwal, Jammu

Undertaking (To be submitted by all Bidders' on their letter head)

We ________________________ (bidder name), hereby undertake that-

- As on date of submission of tender, we are not blacklisted by the Central Government / any of the State Governments / PSUs in India or any Financial Institution in India.
- We also undertake that, we are not involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide / continue the services to bank.

Yours faithfully,

Authorized Signatories

(Name, Designation and Seal of the Company)

Annexure 9-Undertaking of Information Security

(This letter should be on the letterhead of the bidder as well as the OEM/OSD duly signed by an authorized signatory on Information security as per regulatory requirement)

Place:
Date:

General Manager IT,
Head Office, Jammu and Kashmir Grameen Bank.,
Narwal, Jammu

Sir,

Subject: Request for Proposal (RFP) for PFMS Solution as Service

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done)

Yours faithfully,

Authorized Signatory Name:
Designation:

ANNEXURE 10 -Technical Specifications

S.No	Feature	Compliance (Y/N)
1	Solution shall comply with all latest PFMS Guidelines, SOPs, Circulars and Technical Specifications issued by CGA, Ministry of Finance.	
2	Solution shall support all existing and future PFMS APIs/interfaces without requiring major architectural changes.	
3	Vendor shall implement any new PFMS APIs introduced during the contract period without additional licensing cost.	
4	Solution shall support complete Account Validation process.	
5	Solution shall support Name Validation (where applicable).	
6	Solution shall support Aadhaar based validation (if enabled by PFMS/UIDAI).	
7	Solution shall support NPCI Mapper validation wherever applicable.	
8	Solution shall support beneficiary registration, updation and deletion workflows.	
9	Solution shall support scheme mapping as prescribed by PFMS.	
10	Solution shall support bulk beneficiary processing.	
11	Solution shall integrate with Finacle CBS using standard APIs/Web Services/MQ/File interfaces.	
12	Solution shall support REST APIs.	
13	Solution shall support SOAP APIs wherever required.	
14	Solution shall support ISO 20022/XML/JSON formats wherever applicable.	
15	Solution shall support secure SFTP based file exchange.	
16	Solution shall support MQ based messaging.	
17	Solution shall support asynchronous processing.	
18	Solution shall provide API version management.	
19	Solution shall support real-time validation.	
20	Solution shall support batch processing.	
21	Account Validation	
22	Beneficiary Validation	
23	Response Handling	
24	Status Enquiry	

25	Transaction Retry	
26	Duplicate Request Detection	
27	Duplicate Response Handling	
28	Reconciliation Support	
29	Settlement Reports	
30	Exception Handling	
31	TLS 1.2 or higher.	
32	Strong encryption for data in transit.	
33	AES-256 encryption for sensitive stored data.	
34	PKI based certificate authentication.	
35	Digital Signature support.	
36	HSM integration for cryptographic keys.	
37	Role Based Access Control (RBAC).	
38	Maker Checker functionality.	
39	Audit Trail.	
40	Tamper-proof logs.	
41	Password policy configurable.	
42	MFA support for administrative users.	
43	Protection against replay attacks.	
44	Protection against SQL Injection.	

45	Protection against XSS.	
46	Protection against CSRF.	
47	OWASP Top-10 compliance.	
48	Vulnerability Assessment compliance.	
49	Security Audit compliance.	
50	CERT-In advisory compliance.	
51	Support minimum 500 concurrent requests.	
52	Scalable architecture.	
53	Response time less than 2 seconds for validation APIs under normal load.	
54	Queue management mechanism.	
55	Auto Retry mechanism.	
56	High Availability support.	
57	Failover support.	
58	Load balancing support.	
59	Real-time Dashboard.	
60	Transaction Monitoring.	
61	Alert Generation.	
62	SMS/Email alerts.	
63	Health Monitoring.	
64	API Monitoring.	

65	Queue Monitoring.	
66	Account Validation Report	
67	Beneficiary Status Report	
68	Scheme-wise Report	
69	Daily Transaction Report	
70	Monthly MIS	
71	Exception Report	
72	Failure Report	
73	Audit Report	
74	API Usage Report	
75	Reconciliation Report	
76	Complete API logging	
77	Request Response logging	
78	Error logging	
79	Transaction logging	
80	Configurable Log Retention	
81	Centralized Log Management	
82	Disaster Recovery Support	
83	Automatic Backup	
84	Backup Restoration	

85	RPO & RTO compliance	
86	Data Integrity Verification	
87	PFMS SOP compliance	
88	CGA Guidelines compliance	
89	DBT Mission Guidelines compliance	
90	RBI Cyber Security Framework compliance	
91	RBI Digital Payment Security Controls compliance	
92	CERT-In Directions compliance	
93	UIDAI compliance wherever Aadhaar authentication is used	
94	IT Act 2000 compliance	
95	DPDP Act, 2023 compliance	
96	ISO 27001 compliant solution	
97	PCI-DSS compliance wherever payment card data is involved	
98	OWASP secure coding practices	
99	STQC/Third-party security audit support	
100	Compliance with all future PFMS technical changes issued during the contract period without additional licensing cost.	