

JOINT REQUEST FOR PROPOSAL

FOR

Supply, Installation, Implementation, Management and Maintenance of
Enterprise Fraud Risk Management (EFRM) Solution

Jointly Issued by:

UTTAR PRADESH GRAMIN BANK (UPGB)

Head Office: 2nd Floor, NBCC Commercial Complex, Vardan Khand,
Gomti Nagar Extension, Lucknow – 226010, Uttar Pradesh
Website: www.upgb.bank.in | Email: frmc.ho@upgb.bank.in

AND

GUJARAT GRAMIN BANK (GGB)

Head Office: 3rd/4th Floor, Suraj Plaza-1, Sayajiganj,
Vadodara – 390020, Gujarat
Website: www.ggb.bank.in | Email: riskmanagement.ho@ggb.bank.in

GeM Bid Reference	GEM/2026/B/7746645	Date of Issuance	04.07.2026
Joint EMD	₹30,00,000/- (Rupees Sixty Lakhs Only)	Bid Validity	180 Days
Contract Period	Implementation Period + 5 Years (per bank) from Phase 2 Go-live for each bank independently	Evaluation	70% Technical 30% Commercial

JOINT TENDER NOTICE: This RFP is issued jointly by Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB). References to “the Bank” or “the Banks” mean both banks collectively unless specifically qualified as [UPGB] or [GGB]. Bidder must submit one consolidated bid covering both banks’ requirements with bank-wise commercial pricing.

This document is meant for the specific use by the Company/persons interested to participate in the current tendering process. This document in its entirety is subject to Copyright Laws. Both Banks expect the vendors or any person acting on behalf of the vendors to strictly adhere to the instructions given in the document and maintain

confidentiality of information. The vendors will be held responsible for any misuse of information contained in the document, and liable to be prosecuted by the Banks in the event that such a circumstance is brought to the notice of the Banks. By downloading the document, the interested party is subject to confidentiality clauses.

Table of Contents:

SCHEDULE [A] IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION..... 6
SCHEDULE [B] GLOSSARY OF TERMS 8
SCHEDULE [C] DISCLAIMER.....14
SCHEDULE [D] GENERAL INFORMATION.....15
SCHEDULE [E] OVERVIEW OF ISSUING BANK.....16

SECTION – I..... 17
REQUEST FOR PROPOSAL (RFP)..... 17

SECTION – II..... 20
INSTRUCTIONS TO BIDDERS..... 20
1. INTRODUCTION..... 20
2. PRE-BID MEETING 20
3. AMENDMENT OF BIDDING DOCUMENTS 20
4. TECHNICAL BID 20
5. COMMERCIAL BID 20
6. BID SECURITY (EARNEST MONEY DEPOSIT)..... 21
7. BID VALIDITY..... 21
8. COST OF BID DOCUMENT 21
9. ELIGIBILITY CRITERIA..... 21
10. GENERAL EVALUATION CRITERIA..... 24
11. EVALUATION [PROCESS- FOUR STAGE](#) 25
12. STAGE-2 TECHNICAL EVALUATION MATRIX..... 25
13. STAGE-3 COMMERCIAL BID EVALUATION GUIDELINES 27
14. STAGE-4 WEIGHTED COMBINED EVALUATION 27
15. BID SECURITY DECLARATION 27
16. PERFORMANCE BANK GUARANTEE 27
17. PROPOSAL PROCESS MANAGEMENT 28
18. SERVICES..... 28
19. RIGHT OF AUDIT AND VERIFICATION..... 29
20. FRAUD AND CORRUPT PRACTICES 29
21. TAXES AND DUTIES 30
22. LEGAL RELATIONSHIP 31
23. POWERS TO VARY OR OMIT WORK 31
24. WAIVER OF RIGHTS 31
25. CONTRACT AMENDMENTS..... 31
26. BANK’S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS 32
27. SYSTEM INTEGRATION TESTING AND USER ACCEPTANCE TESTING:..... 32
28. WARRANTY AND ANNUAL MAINTENANCE CONTRACT 32
29. NON-SHARING OF RESOURCES 33
30. VALIDITY OF AGREEMENT 33
31. DELAY IN THE VENDOR’S PERFORMANCE..... 33
32. VENDOR’S OBLIGATIONS 34
33. TECHNICAL DOCUMENTATION 34

SECTION – III 35
Broad Scope of Work – Enterprise Fraud Risk Management Solution 35
1. ABOUT THE PROJECT 36
2. PROJECT OBJECTIVES 36
3. SCOPE OF WORK-GENERAL REQUIREMENT..... 36
4. PERFORMANCE REQUIREMENT 39
5. FINACLE CBS INTEGRATION (MANDATORY)..... 40
6. DATA SEGREGATION AND MULTI-BANK ARCHITECTURE 40
7. DETAILED FUNCTIONAL REQUIREMENT 41
7.1 COREFRAUD DETECTION ENGINE..... 41
7.2 CUSTOMER PROFILING..... 42
7.3 SCENARIO AUTHORIZING TOOL (RULE ENGINE)..... 43

7.4 CHANNEL SPECIFIC FRAUD SCENARIOS.....	44
7.4.1 UPI & QR TRANSACTION MONITORING.....	44
7.4.2 AEPS TRANSACTION MONITORING.....	44
7.4.3 IMPS MONITORING.....	44
7.4.4 INTERNET/MOBILE BANKING MONITORING.....	44
7.4.5 ATM/DEBIT CARD MONITORING.....	45
7.4.6 CBS/BRANCH TRANSACTION MONITORING.....	45
7.4.7 MONEY MULE / CYBER FRAUD DETECTION (MANDATORY).....	45
7.4.8 ILLITERATE / VULNERABLE CUSTOMER ENHANCED MONITORING (MANDATORY FOR BOTH RRBs).....	45
7.5 AI/ML GOVERNANCE FRAMEWORK (MANDATORY).....	46
7.6 NABARD REGULATORY REPORTING (MANDATORY FOR BOTH BANKS AS RRBs).....	46
7.7 I4C / NCRP INTEGRATION (MANDATORY).....	46
7.8 WATCH LIST MANAGEMENT.....	47
7.9 CASE MANAGEMENT SYSTEM & MIS (CMS).....	47
7.10 DEVICE INTELLIGENCE AND BEHAVIOURAL BIOMETRICS (MANDATORY).....	48
7.11 REPORTING AND DASHBOARDS.....	49
7.12 ADAPTIVE AUTHENTICATION AND RISK-BASED AUTHENTICATION.....	49
7.13 AUDIT TRAIL AND LOG MANAGEMENT.....	49
7.14 TESTING ENVIRONMENT AND RULE SIMULATOR.....	50
8. TECHNICAL ARCHITECTURE REQUIREMENTS.....	50
8.1 ARCHITECTURE PRINCIPLES.....	50
8.2 INFRASTRUCTURE SIZING.....	50
8.3 DC/DR AND BUSINESS CONTINUITY.....	50
8.4 SECURITY ARCHITECTURE.....	50
9. CYBERSECURITY AND COMPLIANCE.....	51
9.1 MANDATORY REGULATORY COMPLIANCE.....	51
9.2 VAPT AND SECURITY TESTING REQUIREMENTS.....	52
9.3 SOFTWARE BILL OF MATERIALS (SBOM) – MANDATORY PER RBI ADVISORY.....	52
9.4 COMPLIANCE WITH IT & IS SECURITY POLICY.....	52
10. IMPLEMENTATION METHODOLOGY.....	53
10.1 IMPLEMENTATION TIMELINE.....	53
10.2 CUTOVER AND MIGRATION.....	54
11. ONSITE TECHNICAL SUPPORT (FMS) – REQUIREMENTS.....	54
11.1 SUPPORT STRUCTURE.....	54
11.2 SCOPE OF L1 SUPPORT.....	55
11.3 SCOPE OF L2 SUPPORT.....	55
11.4 SCOPE OF L3 SUPPORT.....	57
11.5 TRAINING REQUIREMENTS.....	58
12. UPGRADES AND UPDATES.....	58
13. SERVICE LEVEL AGREEMENT (SLA) AND PENALTIES.....	58
13.1 SYSTEM AVAILABILITY SLA.....	58
13.2 RESPONSE TIME SLA.....	59
13.3 INCIDENT RESOLUTION SLA.....	59
13.4 VULNERABILITY REMEDIATION AND AUDIT GAP PENALTIES.....	59
14. CONTRACT TERMS.....	61
14.1 CONTRACT PERIOD.....	61
14.2 PAYMENT TERMS.....	62
14.4 ESCROW ARRANGEMENT.....	62
14.4 SUB-CONTRACTING.....	63
15. DELIVERABLES.....	63
16. LEGAL AND GOVERNANCE PROVISIONS.....	64
16.1 GOVERNING LAW AND JURISDICTION.....	64
16.2 ARBITRATION.....	64
16.3 CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT.....	65
16.4 INTELLECTUAL PROPERTY RIGHTS.....	65
16.5 DATA OWNERSHIP, PRIVACY AND SECURITY.....	66

16.6	AMALGAMATION / RESTRUCTURING CLAUSE	66
16.7	LIMITATION OF LIABILITY	66
16.8	INDEMNITY	67
16.9	FORCE MAJEURE	67
16.10	TERMINATION.....	67
16.11	REPRESENTATION AND WARRANTIES.....	68
16.12	CONFLICT OF INTEREST.....	69
16.13	PRE-CONTRACT INTEGRITY PACT	69
16.14	INSURANCE	71
16.15	COMPLIANCE WITH IT ACT 2000	71
16.16	SOLICITATION OF EMPLOYEES	71
16.17	AMALGAMATION OF SUPPLIER.....	71
16.18	USE OF CONTRACT DOCUMENTS AND INFORMATION.....	71
16.19	INSPECTIONS AND TESTS.....	71
16.20	IMPLEMENTATION OF SERVICES	72
16.21	TERMINATION FOR INSOLVENCY.....	72
16.22	COMPLIANCE WITH STATUTORY AND REGULATORY PROVISIONS	72
16.23	COMPLIANCE WITH POLICY	72
16.24	OTHER TERMS AND CONDITIONS.....	72
16.25	GENERAL TERMS AND CONDITIONS	73
16.26	NO RIGHT TO SET OFF.....	73
16.27	NOTICES AND OTHER COMMUNICATION.....	73
16.28	SUBSTITUTIONS OF TEAM MEMBERS	74
16.29	SEVERABILITY	74
16.30	PUBLICITY.....	74
16.31	TAXES AND DUTIES.....	74
16.32	COVERAGE OF SUCCESSFUL BIDDER UNDER THE EMPLOYEE'S PROVIDENT FUNDS AND MISCELLANEOUS PROVISIONS ACT, 1952.....	74
16.33	DISCLAIMER.....	74
16.34	ACCEPTANCE OF PURCHASE ORDER.....	75
16.35	PATENT RIGHTS.....	75
16.36	BANK'S RIGHT TO ACCEPT OR REJECT ANY BID OR ALL BIDS	75
16.37	LIQUIDATED DAMAGES.....	75
17.	BIDDER GRIEVANCE REDRESSAL MECHANISM.....	76
17.1	DESIGNATED OFFICERS FOR RECEIPT OF GRIEVANCES	76
17.2	TIME LIMIT FOR SUBMISSION OF REPRESENTATION.....	76
17.3	DISPOSAL OF GRIEVANCES	77
17.4	DEBRIEFING OF BIDDERS	77
17.5	NO STAY ON PROCUREMENT PROCESS.....	77
SECTION – IV		78
	BID SUBMISSION INSTRUCTIONS	78
1.	SUBMISSION VIA GEM PORTAL	79
2.	OFFLINE PHYSICAL SUBMISSIONS (TO BOTH BANKS)	79
3.	INSTRUCTIONS FOR BID SUBMISSION	79
4.	TWO-PART BID STRUCTURE.....	79
5.	KEY INSTRUCTIONS FOR BIDDERS.....	80
SECTION – V		81
	TECHNICAL AND COMMERCIAL BID	81
	PART-I : TECHNICAL AND FUNCTIONAL COMPLIANCE MATRIX	82
	PART-II : COMMERCIAL BID FORMAT	83
	TABLE-A : ENTERPRISE LICENSE AND AMC COST	83
	TABLE-B : IMPLEMENTATION, INTEGRATION, AND CONFIGURATION COST.....	84
	TABLE-C : ONSITE TECHNICAL SUPPORT (OTS/FMS) COST	85
	TABLE-D : CHANGE REQUEST / ENHANCEMENT PRICING.....	85
LIST OF ANNEXURES		88

SCHEDULE [A] – IMPORTANT DATES AND INFORMATION ON RFP SUBMISSION

S.No.	Particulars	Timeline
1	Issuance Date of Joint RFP	04.07.2026
2	Last Date for Pre-bid Queries / Clarifications	On or before 13.07.2026 03:00 PM IST. Queries to be submitted in writing via email to frmc.ho@upgb.bank.in (UPGB) and riskmanagement.ho@ggb.bank.in (GGB). Format as per Annexure-XI (Pre-Bid Query Format).
3	Joint Pre-Bid Meeting – Date, Time and Venue	14.07.2026 03:00 PM IST through Virtual mode. Both Banks’ representatives will participate. Bidders willing to participate must submit (max 2 participants) names, contact numbers, designations and email IDs to frmc.ho@upgb.bank.in AND riskmanagement.ho@ggb.bank.in on or before 13.07.2026 03:00 PM IST. The meeting link is below https://teams.microsoft.com/meet/44805607927436?p=kLxv2clVn5l4PBWzeg Queries raised during pre-bid meeting to be submitted in writing by stipulated date. Clarifications and corrigenda, if any, will be published on both Banks’ websites and GeM portal.
4	Last Date of Submission / Closing Date (Online via GeM + Offline Document Submission)	27.07.2026, 03:00 PM IST for both online bid submission (GeM portal) and physical/offline document submission. Physical documents must be delivered by this date and time to addresse below: General Manager, Fraud Risk Management Department, UPGB Head Office, 2nd Floor, NBCC Commercial Complex, Vardan Khand, Gomti Nagar Extension, Lucknow – 226010, UP.
5	Eligibility-cum-Technical Bid Opening Date	27.07.2026 03:30 PM IST
6	Date, Time, and Venue of Presentation & Demo by Shortlisted Bidders	Dates to be intimated separately to shortlisted bidders by email after technical bid evaluation. Bidders not attending the demo/presentation shall be treated as disqualified from Stage 2 evaluation.
7	Opening of Commercial Bids	Commercial bids of only those bidders who have qualified in Stage 2 Technical Evaluation (minimum 70 marks out of 100) will be opened. Date and time to be communicated to technically qualified bidders via email.
8	Online Bid Submission Portal	This RFP will follow the e-Procurement (e-Tendering) process through Government e-Marketplace (GeM) portal – www.gem.gov.in. Bidders must register on GeM before participating. All documents, except those specifically listed for offline submission (Sl.No. 9), must be submitted online through GeM.
9	Documents to be Submitted Physically (Offline Mode)	(a) Joint Bid Security (EMD) of ₹30,00,000/- (Rupees Sixty Lakhs Only): Single Bank Guarantee from a Scheduled Commercial Bank other than UPGB and GGB, covering both banks jointly as beneficiaries. (b) Pre-Contract Integrity Pact (Annexure-V) duly signed and stamped. (c) Proof of online EMD transfer (if remitted electronically). Offline envelopes must be super-scribed with RFP Reference Number, Closing Date/Time, and Bidder’s Name.
10	RFP Coordinator – UPGB	Name: Tarique Noaman Mobile: 8960588072 Email: frmc.ho@upgb.bank.in

S.No.	Particulars	Timeline
11	RFP Coordinator – GGB	Name: Mukul Sharma Mobile: 9571500231 Email: riskmanagement.ho@ggb.bank.in
12	RFP Document Download	Bank Websites: www.upgb.bank.in and www.ggb.bank.in GeM Portal: www.gem.gov.in Corrigenda and clarifications will be published exclusively on both Banks' websites and GeM portal.

NOTE: All dates and timelines are tentative and subject to change. Any changes will be published on both Banks' websites and GeM portal. If a declared holiday falls on any of the above dates, the next working day at the specified time and venue will apply. Time is Indian Standard Time (IST) throughout.

NOTE: Bank will not be responsible for any bid/offer lost or damaged in transit or delivered to incorrect address. Bidders are advised to submit bids well before the closing date and time to avoid last-minute technical issues on GeM portal.

SCHEDULE [B] – GLOSSARY OF TERMS

The following terms are used in this document interchangeably:

- “Banks” or “the Banks” refers collectively to Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB) including all their Branches, Regional Offices, Business Correspondents, and all other units and establishments.
- “[UPGB]” or “Uttar Pradesh Gramin Bank” refers specifically to Uttar Pradesh Gramin Bank, Head Office Lucknow.
- “[GGB]” or “Gujarat Gramin Bank” refers specifically to Gujarat Gramin Bank, Head Office Vadodara.
- “Recipient” / “Respondent” / “Vendor” / “Bidder” / “Applicant” means the entity responding to this Joint RFP document.
- “Selected Bidder” / “Successful Bidder” / “Service Provider” / “Supplier” / “Vendor” means the entity awarded the contract.
- “Contract” or “Master Agreement” means the Master Service Agreement to be executed between the Successful Bidder and both Banks, along with the Bank-specific Statements of Work (SoW-UPGB and SoW-GGB).
- “EFRM Solution” or “EFRMS” means the Enterprise Fraud Risk Management Solution proposed and implemented by the Successful Bidder.
- “OEM” means Original Equipment Manufacturer — the entity that developed and owns the intellectual property of the proposed EFRM solution.
- “OSD” means Original Software Developer.
- “SI” means System Integrator — an entity that may implement an OEM’s solution as their authorised representative.
- “Go-Live” means the date on which the EFRM Solution or specific phase thereof is fully operational in production environment of the respective Bank after all integration, testing, and sign-off obligations are fulfilled.
- “Phase 2 Go-Live” / “Phase 3 Go-Live” refer to the go-live dates for the respective implementation phases as defined in the Scope of Work.
- “SBOM” means Software Bill of Materials.

Other Terms and abbreviations:

S No.	Abbreviations	Description / Full form
1.	AMC	Annual Maintenance Contract
2.	AA	Adaptive Authentication
3.	ATS	Annual Technical Support
4.	AD	Active Directory
5.	API	Application Programming Interface
6.	ATM	Automated Teller Machine
7.	AI	Artificial Intelligence
8.	AePS	Aadhaar enabled Payment System
9.	AMBAR	Name of Banks Private Cloud Infrastructure
10.	AML	Anti-Money Laundering
11.	ACH	Automated Clearing House
12.	AV	Anti-Virus

13.	BG	Bank Guarantee
14.	Bank	Uttar Pradesh Gramin Bank and/or Gujrat Gramin Bank
15.	BBPS	Bharat Bill Payment System
16.	BHIM	Bharat Interface for Money
17.	BOM	Bill of Material
18.	BCP	Business Continuity Planning
19.	CMS	Cash Management services
20.	CD	Compact Disk
21.	CBS	Core Banking Solution
22.	CERTIn	Computer Emergency Response Team India
23.	CSV	Comma Separated Values
24.	CVC	Central Vigilance Commission
25.	CVV	Card Verification Value
26.	CTS	Cheque Truncation System
27.	DAM	Data Base Activity Monitoring
28.	DD	Demand Draft
29.	DI	Delivery Instructions
30.	DIP	Digital Intelligence Platform
31.	DB	Data Base
32.	DOT	Department of Telecommunication
33.	DC	Data Center
34.	DR Site	Disaster Recovery Site
35.	DCMS	Debit Card Management System
36.	DFS	Department of Financial Services
37.	E-Comm	Electronic Commerce
38.	EMD	Earnest Money Deposit
39.	EBP	External Business Partners
40.	EOL	End of Life
41.	EOS	End of Support
42.	EWS	Early Warning Signals
43.	FRMC	Fraud Risk Management Department
44.	FTP	File Transfer Protocol
45.	FY	Financial Year
46.	GDPR	General Data Protection Regulation
47.	GeM	Government e Marketplace

48.	GGB	Gujrat Gramin Bank
49	GST	Goods and Service Tax
50.	GFR	General Financial Rules
51.	GOI	Government of India
52.	GUI	Graphical User Interface
53.	HO	Head Office
54.	HTTPS	Hyper Text Transfer Protocol Secure
55.	HTML	Hypertext Mark-up Language
56.	HR	Human Resources
57.	IMPS	Immediate Payment Service
58.	I4C	Indian Cybercrime Coordination Centre
59.	IEM	Independent External Monitor
60.	IGST	Integrated Goods and Services Tax
61.	INR	Indian Rupee
62.	IP	Integrity Pact
63.	IPV	Internet Protocol Version
64.	IS	Information System
65.	IST	Indian Standard Time
66.	IT	Information Technology
67.	IVR	Interactive Voice Response
68.	IDRBT	The Institute for Development & Research in Banking Technology
69.	ISO	International Organization for Standards
70.	JV	Joint Venture
71.	JVs	Joint Ventures
72.	JSON	Java Script Object Notation
73.	KYC	Know Your Customer
74.	KPI	Key Performance Indicator
75.	KRA	Key Responsibility Area
76.	KYE	Know Your Employee
77.	LD	Liquidated Damage
78.	LAN	Local Area Network
79.	LOI	Letter of Intent
80.	LEA	Law Enforcement Agencies
81.	LLP	Limited Liability Partnership
82.	LMS	Loan Management System

83.	MCC	Merchant Category Codes
84.	MD	Managing Director
85.	MIS	Management Information System
86.	MHA	Ministry of Home Affairs
87.	ML	Machine Learning
88.	MQ	Message Queue
89.	MSE	Micro and Small Enterprises
90.	MSME	Micro Small Medium Enterprises
91.	M2P	Merchant to Person
92.	NACH	National Automated Clearing House
93.	NDA	Non-Disclosure Agreement
94.	NEFT	National Electronic Funds Transfer
95.	NOC	Network Operation Center
96.	NI Act	Negotiable Instruments Act
97.	NPCI	National Payments Corporation of India
98.	OEM	Original Equipment Manufacturer
99.	ODBC	Open Database Connectivity
100.	OS	Operating System
101.	OTP	One Time Password
102.	OTS	Onsite Technical support
103.	OSM	Offsite Monitoring Application
104.	OMNI channel	Bank's Mobile and Internet Banking application
105.	OWASP	Open Web Application Security Project
106.	PAN	Personal Account Number
107.	PA-DSS	Payment Application – Data Security Standard
108.	P2P	Peer to Peer
109.	P2A	Person to Account
110.	P2M	Person to Merchant
111.	PBG	Performance Bank Guarantee
112.	PCI-DSS	Payment Card Industry - Data Security Standard
113.	PDF	Portable Document Format
114.	PKI	Public Key Infrastructure
115.	PII	Personal Identifiable Information
116.	PIM	Privilege Identity Management
117.	PAM	Privilege Access Management
118.	PIN	Personal Identification Number

119.	PO	Purchase Order
120.	POS	Point of Sale
121.	P&L	Profit and Loss
122.	PFMS	Public Financial Management System
123.	PSU	Public Sector Undertaking
124.	PSB	Public Sector Bank
125.	PT	Penetration Testing
126.	QoS	Quality of Service
127.	Q & A	Questions and Answers
128.	QR	Quick Response
129.	RBI	Reserve Bank of India
130.	RDBMS	Relational Database Management System
131.	RESPONDENT	Is one who responds to this RFP document
132.	RFP	Request for Proposal
133.	RFQ	Request for Quote (online)
134.	RPO	Recovery Point Objective
135.	RRB	Regional Rural Bank
136.	RTGS	Real Time Gross Settlement
137.	RTO	Recovery Time Objective
138.	RCA	Root Cause Analysis
139.	SFTP	Secure File Transfer Protocol
140.	SGST	State Goods and Services Tax
141.	SMS	Short Message Service
142.	SOAP	Simple Object Access Protocol
143.	SQL	Structured Query Language
144.	SSO	Single Sign On
145.	SOC	Security Operation Centre
146.	SOP	Standard Operating Procedure
147.	SRS	Software Requirements Specification
148.	SLA	Service Level Agreement
149.	SIT	System Integration Test
150.	SIEM	Security Incident and Event Management
151.	SSH	Secure Shell
152.	SSL	Secure Sockets Layer
153.	STP	Straight Through Processing
154.	SWIFT	Society for Worldwide Interbank Financial Telecommunications

155.	SI	System Integrator
156.	TAT	Turn Around Time
157.	TCO	Total Cost of Ownership
158.	TCS	Tata Consultancy Services
159.	TCP	Transmission Control Protocol
160.	TCP-IP	Transmission Control Protocol - Internet Protocol
161.	TDS	Tax Deducted at source
162.	TLS	Transport Layer Security
163.	TPS	Transactions Per Second
164.	UAT	User Acceptance Testing
165.	UI	User Interface
166.	UPI	Unified Payments Interface
167.	URL	Uniform Resource Locator
168.	VA	Vulnerability Analysis
169.	VPA	Virtual Payment Address
170.	WAN	Wide Area Network
171.	XML	Extensible Mark-up Language
172.	2FA	Two Factor Authentication

Any term used in this document and not specifically defined herein will have the same meaning as provided in relevant RBI regulations and/or RBI/NABARD guidelines. In case of any dispute, the decision of the Banks shall be final and binding.

SCHEDULE [C] – DISCLAIMER

The information in this Joint Request for Proposal (“RFP”) document provided to bidders or applicants, whether verbally or in documentary form by or on behalf of Uttar Pradesh Gramin Bank (UPGB) and/or Gujarat Gramin Bank (GGB), is under the terms and conditions set out in this RFP document.

This Joint RFP document is not an agreement, offer, or an invitation by either Bank to enter into an agreement or contract in relation to the service described herein. It is designed to assist applicants/Bidders in formulating their proposals and does not claim to contain all information that may be required by them.

Each Bidder may conduct its own independent investigation and analysis and is free to check the accuracy, reliability, and completeness of the information in this RFP. Neither Bank, nor their respective directors, officers, employees, agents, or advisors make any 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 information in this RFP is selective and is subject to updating, expansion, revision, and amendment. It does not purport to contain all information that a Bidder may require. Neither Bank undertakes to provide any Bidder with access to additional information or to update the information in this RFP or to correct inaccuracies that may become apparent.

Bidders, by accepting this document, agree that any information contained herein may be superseded by any subsequent written information on the same subject communicated to bidders or published on either Bank’s website and/or on the GeM portal. It is understood and agreed that the decision of the Banks regarding selection of the Bidder will be final and binding on all concerned. No correspondence in this regard, verbal or written, will be entertained.

It shall be the duty and responsibility of the Bidders to ensure their legal, statutory, and regulatory eligibility and competency to participate in this RFP process and to provide all the services and deliverables as specified herein.

The Bidder shall bear all costs associated with preparation and submission of its bid, including preparation, copying, postage, delivery, and any demonstrations or presentations required by the Banks. Neither Bank shall be liable in any manner for costs or expenses incurred by the Bidder in connection with the preparation or submission of the bid.

Both Banks, in their absolute discretion, but without being under any obligation, may update, amend, or supplement the information in this RFP. Such changes will be published on both Banks’ websites and on the GeM portal, and will become part and parcel of this RFP.

Both Banks jointly reserve the right to reject any or all bids/proposals received in response to this RFP at any stage without assigning any reason whatsoever. The decision of both Banks in this regard shall be final, conclusive, and binding on all parties.

△IMPORTANT: Neither Bank is under any obligation to proceed with this procurement process. The Banks reserve the right to cancel or postpone this tender at any stage without liability to any Bidder.

SCHEDULE [D] – GENERAL INFORMATION

This Joint RFP is issued on behalf of both Banks by their respective Risk Management / Fraud Risk Management Departments. All communications, queries, and submissions should be directed to both coordinators as specified in Schedule [A].

Both Banks follow a Two-Bid System. Part-I (Technical Bid) shall contain compliance details of the eligibility and technical specifications. Part-II (Commercial Bid) shall be submitted separately. Technical bids of all eligible Bidders will be evaluated, and only technically qualified Bidders will be invited for commercial bid opening.

Bidders must register on the Government e-Marketplace (GeM) portal (www.gem.gov.in) before participating. All documents, except those required for offline submission listed in Schedule [A], must be submitted through GeM. Documents submitted by any other mode will not be accepted.

All documents uploaded online must be duly signed by the Authorised Signatory under the seal of the bidder company/firm on every page. Any correction must be authenticated by the same signatory. Insufficient, false, or misleading information and any deviation from stipulated terms and conditions shall render the bid liable for rejection.

Prices quoted must be unconditional and must not contain any strings attached. Bids that do not conform to eligibility criteria and terms and conditions are liable for rejection. The RFP document and addenda must be signed and stamped by the authorised signatory and submitted with the Technical Bid as evidence of having read and understood the contents.

SCHEDULE [E] – OVERVIEW OF ISSUING BANKS

E.1 Uttar Pradesh Gramin Bank (UPGB)

Uttar Pradesh Gramin Bank (UPGB) was established on May 1, 2025 through the amalgamation of Aryavart Bank, Baroda UP Bank, and Prathama UP Gramin Bank under the Government of India's "One State One RRB" initiative. UPGB is a Scheduled Bank owned by the Government of India, sponsored by Bank of Baroda, and is one of the largest Regional Rural Banks in India.

Parameter	Details
Head Office	2nd Floor, NBCC Commercial Complex, Vardan Khand, Gomti Nagar Extension, Lucknow – 226010, Uttar Pradesh
Branch Network	4,329 Branches
Regional Offices	65
Business Correspondents	12,000+
Customer Base	Approximately 8 Crore (80 million)
Total Business (March 2026)	₹2.16 Lakh Crore
CBS Platform	Finacle
Website	www.upgb.bank.in
RFP Contact Email	frmc.ho@upgb.bank.in

E.2 Gujarat Gramin Bank (GGB)

Gujarat Gramin Bank (GGB) was established on May 1, 2025 through the amalgamation of Baroda Gujarat Gramin Bank and Saurashtra Gramin Bank, as part of the Government of India's "One State One RRB" initiative. GGB is a Scheduled Bank owned by the Government of India, sponsored by Bank of Baroda.

Parameter	Details
Head Office	3rd/4th Floor, Suraj Plaza-1, Sayajiganj, Vadodara – 390020, Gujarat
Branch Network	745 Branches
Regional Offices	13
Business Correspondents	2,400+
Customer Base	Approximately 74 Lakh
Total Business (March 2026)	₹47,605 Crore
CBS Platform	Finacle
Website	www.ggb.bank.in
RFP Contact Email	riskmanagement.ho@ggb.bank.in

SECTION – I: REQUEST FOR PROPOSAL (RFP)

Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB), both Regional Rural Banks constituted under the Regional Rural Banks Act, 1976, and regulated by the Reserve Bank of India (RBI) and supervised by NABARD, hereby jointly invite proposals from eligible and experienced firms/companies for the “**Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (EFRM) Solution**” as specified in this RFP.

Both Banks are offering various delivery channels to their customers and, therefore, it is imperative that a robust EFRM Solution be implemented that is capable of:

- Supporting the prevention, detection, analytics, and management of frauds across user profiles, accounts, products, processes, and channels in real-time.
- Monitoring, analysing user activity, behaviour, and trends at the application level in order to observe what transpires inside and across customer accounts, using any/all banking channels available to the user.
- Analysing behaviour among related users, accounts, customer profiles, or other entities, looking for organised criminal activity, fraud rings, money mule networks, corruption, or misuse.
- Providing a combination of highly complex algorithms, sophisticated system architecture and design for optimum data flow, AI/Machine Learning models for predictive analysis, coupled with the best computer engineering design for real-time transaction monitoring with millisecond response times.
- Detecting, investigating, and preventing fraud across all delivery channels – online, mobile, ATM, UPI, AEPS, CBS, IMPS, NEFT/RTGS, BBPS, and others.
- Reducing fraud losses by improving the accuracy and efficiency of fraud detection while minimising false positives and false negatives.
- Enhancing regulatory compliance by ensuring adherence to RBI, NABARD, DFS, CERT-In, and DPDP Act requirements.
- Improving operational efficiency by streamlining fraud risk management processes and enabling automated regulatory reporting.

Both Banks will follow a two-bid system. Part-I (Technical Bid) shall contain compliance details. Part-II Commercial Bid with price breakup details to be submitted separately along with the bid documentation. All bids must be submitted through the GeM portal. Physical submission of select documents is required at both Banks’ offices as specified in Schedule [A].

Interested eligible Bidders may submit their Bid for the above solution as specified in this RFP. The evaluation process will be carried out by a Joint Technical Evaluation Committee comprising representatives of both Banks. Award of contract will be made to the H-1 Bidder (highest combined techno-commercial score), who will then execute independent contracts with each Bank.

RESTRICTION OF BIDDERS FROM COUNTRIES SHARING LAND BORDERS WITH INDIA:

As per Ministry of Finance, Department of Expenditure, Public Procurement Division’s office memorandum F.No.6/18/2019-PPD dated 23.07.2020, regarding insertion of Rule 144 (xi) in the General Financial Rules (GFR) 2017, any bidder from a country which shares a land border with India will be eligible to bid either as a single entity or as a member of a JV / Consortium with others (for JV/consortium, refer eligibility criteria), in any procurement whether of goods, services (including consultancy services and non- consultancy services) or works (including turnkey projects) only if the bidder is registered with the Competent Authority. The Competent Authority for registration will be the Registration Committee constituted by the Department for Promotion of **Joint RFP for EFRM solution for UPGB and GGB**

Industry and Internal Trade (DPIIT). Political & Security clearance from the Ministries of External and Home Affairs respectively will be mandatory.

However, above condition shall not apply to bidders from those countries (even if sharing a land border with India) to which the Government of India has extended lines of credit or in which the Government of India is engaged in development projects. Updated lists of countries to which lines of credit have been extended or in which development projects are undertaken are given in the website of the Ministry of External Affairs (MEA).

“The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority”

Definitions pertaining to “Restriction of Bidders from Countries sharing Land Borders with India” Clause “Bidder” (including the term 'tenderer', 'consultant' 'vendor' or 'Service Provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated herein before, including any agency, branch or office controlled by such person, participating in a procurement process.

"Bidder from a country which shares a land border with India" means:

- a) An entity incorporated, established or registered in such a country; or
- b) A subsidiary of an entity incorporated, established or registered in such a country; or
- c) An entity substantially controlled through entities incorporated, established or registered in such a country; or
- d) An entity whose beneficial owner is situated in such a country; or
- e) An Indian (or other) agent of such an entity; or
- f) A natural person who is a citizen of such a country; or
- g) A consortium or joint venture where any member of the consortium or joint venture falls under any of the above

"Beneficial owner" will be as under:

- a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation – For the purpose of this sub-clause:

- "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company.
 - "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholder's agreements or voting agreements.
- b. Where the customer is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership or who exercises control through other means.

Explanation – For the purpose of this sub-clause, "control" shall include the right to control the management or policy decision.

- c. Where the customer is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation — Term "body of individuals" includes societies. Where no natural person is identified under (a), (b), or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

- d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

"Agent" is a person employed to do any act for another, or to represent another in dealings with third persons.

2. Please note that

- (i) The cost of preparing the bids, including visit / visits to the Bank is not reimbursable.
- (ii) Each recipient should notify the Bank of any error, fault, omission, or discrepancy found in this RFP document but not later than last date of receiving clarifications.
- (iii) The Bank is not bound to accept any of the bids submitted and the bank has the right to reject any/all bid/s or cancel the tender at any point without assigning any reason thereof.
- (iv) All pages of the Bid document, Clarifications/Amendments, if any, should be signed by the Authorized Signatory under the seal of the Bidder Company / firm and to be uploaded with technical bid. A certificate to the effect that the Authorized Signatory has authority to bind the company/ firm should also be attached along with the technical bid.
- (v) The Authority/Bank shall not be liable for any omission, mistake or error in respect of any of the above or on account of any matter or thing arising out of or concerning or relating to RFP, Bidding Documents or the Bidding Process, including any error or mistake therein or in any information or data given by the Authority.
- (vi) Nothing in this RFP shall obligate either Party to enter into any further Agreements.

After technical evaluation, intimation will be given to all technically qualified bidders about the date and time of opening of commercial bids.

Note: The tender cannot be split.

SECTION – II: INSTRUCTIONS TO BIDDERS

1. Introduction

The Bidder is expected to examine all instructions, forms, terms, and specifications given in the Bidding Documents. If any element of doubt arises, the same should be clarified from both Banks through the mechanism specified herein. Failure to furnish all information required in the Bidding Documents may result in rejection of the bid, which will be at the Bidder's own risk. Neither Bank shall be responsible for any consequences arising from inadequate or incorrect submissions.

2. Pre-Bid Meeting

- A joint pre-bid meeting will be held on the date and time specified in Schedule [A], conducted virtually, with representatives of both Banks participating.
- Maximum two (2) authorised representatives per Bidder may attend the pre-bid meeting.
- Bidders must register by email to both Bank coordinators by the deadline in Schedule [A], providing participant names, designations, contact numbers, and email IDs.
- The purpose of the pre-bid meeting is to clarify doubts raised by probable Bidders. Queries must be submitted in writing in the format at Annexure-XI before the stipulated query deadline.
- Minutes of the pre-bid meeting, including clarifications (without identifying the source of queries), and any corrigenda, will be published on both Banks' websites and GeM portal.
- Non-attendance at the pre-bid meeting shall not be a cause for disqualification.

3. Amendment of Bidding Documents

- At any time prior to the bid submission deadline, either Bank, for any reason, whether at its own initiative or in response to clarifications requested by Bidders, may modify the Bidding Document.
- All amendments and clarifications will be published on both Banks' websites and GeM portal and shall form part of the Bidding Document.
- All email communications regarding this RFP must be addressed to both Bank coordinators simultaneously.
- No bid submitted under this RFP can be withdrawn or modified after the last date for bid submission, unless specifically permitted in writing by both Banks.

4. Technical Bid

The Bidder shall furnish as part of its Technical Bid all documents establishing the Bidder's eligibility and qualifications to perform the Contract. The Technical Bid must establish to both Banks' satisfaction that the Bidder has the financial and technical capability necessary to perform the Contract. Any bid not accompanied by all required documents shall be rejected.

5. Commercial Bid

- Commercial bids will be opened only after evaluation of Technical Bids and notification to technically qualified Bidders.
- The Bidder must submit the overall pricing for UPGB and GGB within the consolidated Commercial Bid.
- Calling of bids does not confer any right on a Bidder for being awarded any purchase order.

6. Bid Security (Earnest Money Deposit – EMD)

6.1 The Bidder shall submit, as part of its bid, a Joint Bid Security (EMD) of ₹30,00,000/- (Rupees Thirty Lakhs Only) in the form of a Bank Guarantee issued by a Scheduled Commercial Bank (other than UPGB and GGB, and other than cooperative banks) located in India, naming both UPGB and GGB jointly as beneficiaries. The Bank Guarantee must be valid for a minimum of 210 days from the last date of bid submission.

6.2 The EMD may be forfeited/Bank Guarantee invoked if:

- The Bidder withdraws or modifies its bid during the period of bid validity.
- The Bidder makes any false, incorrect, or misleading statements or conceals material information at any time prior to contract signing.
- The Selected Bidder fails or refuses to sign the contract within the specified time from the date of issue of Purchase Order.
- The Selected Bidder fails or refuses to furnish Performance Bank Guarantees in the required form and manner.
- The Bidder violates any provisions of the terms and conditions of this RFP.
- In case any of the above criteria, the Bidder may be suspended from participating in both Banks' tenders for a period of 2 years.

6.3 The EMD of unsuccessful Bidders will be returned/discharged within 30 days of award of contract. The EMD of the Successful Bidder will be returned upon execution of the contract and furnishing of Performance Bank Guarantees by both Banks.

6.4 MSEs/Startups as per GOI policy are eligible for exemption from EMD on submission of relevant MSME/Udyam registration certificates and a Bid Security Declaration in the prescribed format.

7. Bid Validity

Bids shall remain valid for 180 days from the last date of bid submission. In the event the last date is extended, bid validity shall be reckoned from the revised date. The Banks may request an extension of bid validity, and Bidders are expected to comply.

8. Cost of Bid Document

Not applicable for this RFP, which is conducted via GeM portal. Tender Fee: Nil.

9. Eligibility Criteria

Both Banks are looking for eligible Bidders who fulfil the following mandatory criteria. Offers received from Bidders not fulfilling ANY ONE of the following criteria are liable for rejection. Non-compliance with any criterion shall result in disqualification at Stage 1.

S.No.	Criterion	Documentation Required
1	The bidder must be registered in India as Company/PSU/PSE/Proprietorship/Partnership/LLP. In operation minimum 5 years as of RFP date.	Certificate of Incorporation issued by Registrar of companies and full address of the registered office along with copies of MOA/AOA or Partnership Deed along with GST registration certificate.
2	The Bidder is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017. (or) The Bidder is from such a country and has been registered with the Competent Authority i.e. the Registration Committee constituted by the Department for Promotion of Industry and Internal	Undertaking on letterhead. DPIIT registration certificate if applicable. (Annexure-VIII)

S.No.	Criterion	Documentation Required
	Trade (DPIIT), as stated under Annexure to the said Office Memorandum / Order and we submit the proof of registration herewith.	
3	<p>The bidder must be OEM/OSD or Authorised Indian Representative. No consortium bids. The bidder must have an average turnover of minimum Rs 12 cr during last 03 (three) financial years i.e FY'23-24, FY'24-25 and FY'25-26.</p> <p>For MSEs/Startups (as per above point 6.4) an average turnover of minimum Rs. 6 Cr during last 03 (three) financial years i.e. FY 23-24, FY 24-25 and FY 25-26.</p>	<p>In case of authorized representative / partner of the primary product, MAF from OEM as per Annexure-XIX in their letter Head needs to be provided. (Name, designation, contact no & official mail id of the signing authority must be clearly mentioned in the MAF.)</p> <p>In case bidder itself is OEM of the EFRM Solution, undertaking as per Annexure- XX on their company's letter head should be provided.</p> <p>Provide CA Certificate as per Annexure- XIII and Audited Financial statements (Balance sheet and Profit & Loss statement) for three (3) financial years. The CA certificate provided in this regard should be without any riders or qualification.</p> <p>If the bidder is already working in a Scheduled Public/Private sector Bank in India and is a wholly owned subsidiary of a global OEM/OSDs operating in India, the global turnover may be considered for the last 3 financial years viz. 2026, 2025 and 2024 subject to an unconditional undertaking from the Parent Company for completion of the proposed project, in case the bidder (wholly owned Indian subsidiary) defaults or fails to honour the RFP/Contract.</p>
4	<p>The bidder should be profitable organization on the basis of profit after tax (PAT) for at least 02 out of last 03 financial years mentioned in para 3 above.</p> <p>The net worth of the Bidder should not be negative on 31.03.2026 and also net worth should have not eroded by more than 30% (thirty per cent) in the last three years ending on 31.03.2026.</p>	<p>Self-attested Copies of audited financial statements duly certified by auditor along with the auditor's report to be enclosed. Along with the net worth certificate for last three years ending 31.03.2026.</p> <p>If the bidder is already working in a Scheduled Public/Private sector Bank in India and is a wholly owned subsidiary of a global OEM/OSDs operating in India, the global net worth may be considered for the last 3 financial years viz. 2026, 2025 and 2024 subject to an unconditional undertaking from the Parent Company for completion of the proposed project, in case the bidder (wholly owned Indian subsidiary) defaults or fails to honour the RFP/Contract.</p>
5	Bidder and OEM not debarred/blacklisted by Govt. of India / State Governments / Regulatory Agencies / PSUs / other institutions at the time of submission of bid and Bidder not insolvent, bankrupt, in receivership, or being wound up.	Self-Declaration (Annexure -II).
6	Bidder/OEM/OSD in EFRM software business for minimum 5 years as of bid date. In case of the	PO copies and Go-live / satisfaction letters from clients.

S.No.	Criterion	Documentation Required
	OEM/Bidder is MSME/Startup the experience required is 3 years as on 31.03.2026.	
7	Proposed solution / transaction monitoring system live at minimum 2 Scheduled Commercial Banks / RRB in India. One ≥1,500 branches; one ≥1,000 branches. Solution should be in both banks, Live ≥2 years as of 31.03.2026.	Self-declaration / OEM / OSD letter with name of banks and supporting document issued by other banks / PO copy can be provided in support along with Annexure-XII .
8	Bidder/OEM should have integrated experience EFRM solution / transaction monitoring system with minimum 3 channels out of following mentioned channels in single implementation: <ol style="list-style-type: none"> 1. CBS 2. Internet Banking 3. Mobile Banking 4. Debit card 5. UPI (mandatory) 6. AEPS Note: The above clauses are for eligibility purpose only. Bank requires an implementation in real time preventive mode and integration at an enterprise level mandatorily for all the above mentioned channels as well as other channels mentioned elsewhere in the RFP.	Self-declaration / OEM / OSD letter with name of banks and supporting document issued by other banks / PO copy can be provided in support along with Annexure-XII .
9	OEM has development & support centre in India with ≥150 technical resources on payroll.	OEM certificate on letterhead mentioning centre addresses and headcount.
10	Bidder (who is an authorized representative of OEM) has development & support centre in India with ≥100 technical resources on payroll (including Architecture, Development, Testing, Business Analysis roles).	Undertaking on Bidder letterhead with addresses and headcount.
11	Certification requirements: The Bidder should possess any three (3) of the below certifications which are valid at the time of bidding: <ol style="list-style-type: none"> 1. Valid ISO 9001:2008/ISO 9001:2015 for quality management system 2. ISO 20000:2011/ISO 20000-1:2018 for IT service management 3. ISO 27001:2022 for Information Security Management system 4. CMMi Level 3 or above for capability Maturity Model Integration 5. PCI – DSS-4.0 	Copy of valid certificate.
12	Bidder should have all necessary licences, GST registration, PAN, and statutory approvals as required under the law for carrying out its business. It should have valid GST and other applicable taxes registration certificates/PAN etc.	Undertaking + registration copies.
13	Bidder must provide information that any of its subsidiary or associate or holding company or companies having common director/s or companies	Self-undertaking on company letterhead.

S.No.	Criterion	Documentation Required
	in the same group of Promoters/ management or partnership firms/LLPs having common partners have not participated in the bid process.	
14	Labour Law compliance.	CA/Statutory Auditor certificate or self-undertaking.
15	Bidder and OEM undertaking that ALL technical and functional features in the Scope of Work are available in the proposed solution.	Undertaking on letterhead (Annexure — XV)

Note:

- This RFP does not permit consortium or JV bids. The JV/Consortium language in the border-country restriction section should be retained as a standard Gol clause but qualified with a note that it applies to the extent JV bids are permitted, which they are not in this RFP.
- Attested photocopies of all relevant documents / certificates should be submitted as proof in support of the claims made. The bidder should provide relevant additional information wherever required in the eligibility criteria. The Bank reserves the right to verify /evaluate the claims made by the Bidder independently. Any decision of the Bank in this regard shall be final, conclusive and binding upon the Bidder.
- Either the Bidder on behalf of the OEM/OSD or the OEM/OSD themselves can participate in the bid, but both cannot bid simultaneously for the same solution.
- Proposed EFRM Solution should be latest version and no older version to be proposed by the OEM/Bidder.
- No change/ addition / deletion to be made by the Bidder to any of the clauses. In case any such modification is observed in words / sentence / clause in any of the Bank's standard clauses or documents or formats, and noticed by the Bank at any stage, the Bidder may be liable for disqualification / termination, and in such case, EMD / PBG could be forfeited, at the sole discretion of the Bank.
- Non-financial transactions include, but not limited to: Balance Enquiry, Pin/Password change, mini statement, add beneficiary/payee, failed /pass login etc.

Documentary evidence must be furnished against each of the above criteria along with an index. All documents must be signed by the authorized signatory (Copy of Board Resolution or Power of Attorney authorising the signatory to participate in the bid on behalf of the company to be provided) of the Bidder. Relevant portions, in the documents submitted in pursuance of eligibility criteria, should be highlighted.

10. General Evaluation Criteria

All bids will be evaluated by a Joint Evaluation Committee constituted by both Banks. Banks will review each bid for completeness, proper signing, and compliance with bid requirements. Minor informalities that do not materially deviate from terms may be waived by the Banks.

The evaluation will be based on Techno-Commercial scoring: Technical Weightage 70% and Commercial Weightage 30%. The combined weighted score determines the Successful Bidder.

Bidders must fully comply with ALL eligibility criteria (Section II, Para 9), ALL mandatory specifications in the Functional and Technical Specifications (Section III), and all other mandatory provisions of this RFP. Failure to comply with any one or more criteria will result in disqualification.

11. Evaluation Process – Four Stage

Stage	Description	Outcome
Stage 1	Technical Qualification: Pass/Fail evaluation of all Eligibility Criteria (Para 9) and compliance with ALL mandatory Functional & Technical Specifications.	Qualified Bidders proceed to Stage 2.
Stage 2	Technical Evaluation: Scoring on 100-point matrix (Para 12). Minimum qualifying score: 70 marks out of 100.	Qualified Bidders (score ≥ 70) invited for Commercial Bid opening.
Stage 3	Commercial Evaluation: Commercial bids opened and evaluated. Lowest evaluated combined TCO identified.	All commercially valid bids proceeded for weighted evaluation.
Stage 4	Weighted Combined Evaluation: Technical Score (70%) + Commercial Score (30%) = Combined Score. H-1 Bidder recommended for award.	H-1 Bidder awarded contract by both Banks.

12. Stage 2 – Technical Evaluation Matrix

S.No.	Evaluation Parameter	Evidence Required	Max Marks
1	Functional & Technical Specification Compliance Score (Stage 1 score, proportionately scaled). <ul style="list-style-type: none"> Available Out-of-the-Box = 1; Not available or Available through customisation before Go-Live= 0 Not available= 0 (Disqualified) Minimum 85% compliance for qualification.	Completed Functional & Technical Compliance Matrix (Annexure-XV).	35
2	Bidder / OEM should have implemented one of the following solutions in at least 2 Schedule Commercial Banks/RRB. Bidders experience <ol style="list-style-type: none"> Enterprise wide Fraud Risk Management Solution (EFRM) Real-time Transaction Monitoring Non-Real-time Transaction Monitoring Universal / Unified Case Manager Device Fingerprinting / Behavioral Biometrics Mule Identification AI/ML-based Fraud or Risk Models Customer Peer Profiling, Device Profiling and Transaction Profiling Data Analytics Platform Marks shall be allotted as given below: <ol style="list-style-type: none"> 5 Banks = 10 marks 4 Banks = 8 marks 	Performance Certificates / Reference Letters / PO copies / Go-Live Certificates from reference banks.	10

S.No.	Evaluation Parameter	Evidence Required	Max Marks
3	<p>3. 3 Banks = 6 Marks 4. 2 Banks = 4 Marks</p> <p>EFRM Solution live in Scheduled Commercial Banks/RRB in India. AND all 5 mandatory channels live in real-time.</p> <ol style="list-style-type: none"> 1. Mobile Banking 2. Internet Banking 3. UPI 4. Debit Card 5. AEPS 6. CBS <p>3 or more qualifying sites: 10 marks. 2 qualifying sites: 5 marks. 1 qualifying site: 3 marks.</p>	Performance Certificates / Reference Letters / PO copies / Go-Live Certificates from reference banks.	10
4	Channel Integration Depth: In the best qualifying reference site, first 6 mandatory channels (Mobile Banking, Internet Banking, UPI, Debit Card, AEPS, CBS) must be integrated in real-time as prerequisite. Each additional channel beyond the 6 mandatory = 1 mark. 10+ channels in real-time = 10 marks.	Client reference letter with channel-wise integration confirmation. Subject to site visit verification.	10
5	<p>High-Volume Production Deployment: Number of Scheduled Commercial Banks/RRB where solution is live at ≥1,500 TPS.</p> <ul style="list-style-type: none"> • 1 SCB/RRB with ≥1,500 TPS: 5 marks. • 2 or more SCBs/RRB with ≥1,500 TPS: 10 marks. 	Bank certificates confirming live TPS performance.	10
6	<p>Presentation & Demo by Bidder (evaluated by Joint Technical Evaluation Committee):</p> <ol style="list-style-type: none"> (a) Rule Engine and case manager – 5 marks; (b) Live Fraud Scenario Demo (UPI fraud, Mule detection, I4C integration, Device Intelligence, FRI/MNRL) – 5 marks; (c) AI/ML Governance Framework, Model Risk Register, Explainability – 5 marks; (d) Implementation Plan, Integration Strategy– 5 marks; (e) Security Architecture, VAPT compliance, SBOM, DCP, Data Segregation demo – 5 marks. 	Live working demo of the proposed solution. Bidder must showcase claimed features in real-time. Mere presentation without demo shall be penalised in scoring.	25
TOTAL			100

NOTE: Minimum Stage 2 qualifying score is 70 marks. Bidders scoring below 70 are eliminated and their commercial bids are returned unopened. Banks' decision on technical scoring is final and binding.

13. Stage 3 – Commercial Bid Evaluation Guidelines

- Commercial bids of all Stage 2 qualified Bidders (score ≥70) will be opened simultaneously.
- Bidders must quote joint pricing for UPGB and GGB within the consolidated bid format (Annexure-XVI Commercial Bid).
- All prices in Indian Rupees (INR). Fixed price basis. No price escalation permitted during contract or extension period.
- Prices must be inclusive of all costs: software, license, implementation, integration, ATS, OTS, training, escrow, documentation, travel, taxes including GST. Oracle license costs excluded from GGB pricing.
- Prices must not be linked to any foreign exchange rates, commodity prices, or external variables.
- Commercial bids with arithmetic errors will be rectified: unit price prevails over extended amount; words prevail over figures. Bidders not accepting correction will be rejected.
- Any contradictory information, conditional pricing, missing items in TCO computation, or computational errors may lead to disqualification at the sole discretion of both Banks.
- The Banks may conduct Reverse Auction for commercial bids of qualified Bidders, if deemed appropriate.

14. Stage 4 – Weighted Combined Evaluation

The Combined Score is calculated using the formula:

$$H = (T / T_High \times 70) + (C_Low / C \times 30)$$

Where: H = Combined Score of the Bidder; T = Aggregate Technical Score of the Bidder; T_High = Highest Aggregate Technical Score among all Bidders; C = Total Commercial Quote of the Bidder (UPGB TCO + GGB TCO combined); C_Low = Lowest Total Commercial Quote among all Bidders. Bidders shall be ranked H-1, H-2, H-3, etc. based on combined score. The Bidder with the highest combined score (H-1) shall be recommended for award of contract. In case of a tie, the Bidder with the higher Aggregate Technical Score shall be declared H-1.

Example

Bidder	Aggregate Technical Score (T)	Nominal Bid Price in INR (C)	Technical Weightage (T1)	Commercial Weightage (C1)	Combined Score (out of 100) H= T1 + C1
A	95	271	95/95*70=70.00	260/271*30=28.78	70.00+28.78=98.78 (H-1)
B	85	265	85/95*70=62.63	260/265*30= 29.43	62.63+29.43=92.06 (H-2)
C	80	260	80/95*70=58.94	260/260*30=30	58.94+30.00=88.94 (H-3)

15. Bid Security Declaration

MSE/Startup Bidders eligible for EMD exemption must submit a Bid Security Declaration (Annexure-XIV) as per prescribed format in lieu of EMD. In case of withdrawal/modification of bid during validity period, or failure to execute contract after award, the Bid Security Declaration will be invoked and the Bidder may be suspended from participating in both Banks’ tenders for a period of 2 years.

16. Performance Bank Guarantee

Within 30 days of issue of Purchase Order, the successful bidder shall furnish to the each Bank **Joint RFP for EFRM solution for UPGB and GGB**

the Performance Security equivalent to 5% of the contract value in the form of a Bank Guarantee from a scheduled commercial Bank located in India, valid for up to the contractual period plus 60 days, in the format enclosed ([Annexure-IV](#)). Relaxation if any, extended by GOI / competent authorities for furnishing PBG shall be passed on to eligible bidders. In case the contract is being extended beyond 72 months with successful bidder then Successful bidder has to submit PBG on pro rata basis.

The performance security submitted by the successful bidder shall be invoked by the Bank as compensation for any loss resulting from the bidder's failure in completing their obligations or any other claim under the Contract after cure period of 90 days.

The performance security will be discharged by the Bank and returned to the successful bidder not later than thirty (30) days following the date of completion of the successful performance obligations under the Contract.

Failure of the successful bidder to comply with the requirement of signing of contract and providing performance security shall constitute sufficient grounds for annulment of the award and forfeiture of the bid security, in which event the Bank may call for new bids.

17. Proposal Process Management

- Banks reserve the right to accept or reject any bid or all bids and to annul the bidding process at any time prior to contract award, without incurring any liability to affected Bidders.
- Banks reserve the right to modify terms and conditions of this RFP before bid submission deadline, with notification on both Banks' websites and GeM portal.
- Banks reserve the right to waive minor informalities, non-conformities, or irregularities that do not constitute material deviation.
- Canvassing, lobbying, or influence of any kind shall result in disqualification.
- The Tender/Bid cannot be split. The Successful Bidder must implement the solution for both Banks.

18. Services

- i. Bidder should ensure that the quality of methodologies for delivering the services, adhere to quality standards/timelines stipulated therefor.
- ii. Bidder shall provide and implement patches/ upgrades/ updates for software as and when released or as per requirements of the Bank, with no extra cost to the Bank. Bidder should bring to the notice of the Bank all releases/ version changes.
- iii. The bidder shall obtain written permission from the Bank before applying any of the patches/ upgrades/ updates. Bidder must support older versions of the hardware/ software/ operating system/middleware etc. in case the Bank chooses not to upgrade to the latest version. During the entire period, the Bidder must undertake comprehensive support of the product or specified hardware/software and all new versions, releases, and updates for all standard products or specified hardware/software that needs to be installed at no additional cost.
- iv. Bidder shall provide maintenance support for software over the entire period of the contract.
- v. The selected Bidder shall support the product or specified software during the period of the Contract as specified in the Scope of Work in this RFP.
- vi. During the support period, the Bidder shall maintain the product or specified software to comply with the parameters defined in this RFP. The Bidder shall be responsible for all costs relating to labour, spares, maintenance (preventive and corrective), compliance with security requirements, and transport charges from and to the Site(s) in connection with the repair/ replacement of product and ensure continuity of service.
- vii. During the support period, the vendor shall ensure that services of professionally qualified personnel are available for providing continuity in services at sites as per the Bank's

requirements. Continuity of Services shall include, among other things, day-to-day maintenance of the premises or software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging and configuring facility as per the requirements of the Bank, fine-tuning, system monitoring, log maintenance, etc. The Bidder shall provide services of expert technical support at Bank's DC and DR sites, whenever it is essential.

- viii. In the event of product or specified hardware/software breakdown or failures at any stage, protection available, which would include the following, shall be specified.
 - a. Diagnostics for identification of product or specified hardware/software failures
 - b. Protection of data/configuration
 - c. Recovery/restart facility
 - d. Backdrop of product or specified hardware/software/configuration
- ix. Prompt support shall be made available as desired in this RFP during the support period at the locations as and when required by the Bank.
- x. The Bidder shall be agreeable to on-call/on-site support during peak weeks (the last and first week of each month) and at the time of switching over from DC to DR and vice-versa. No extra charge shall be paid by the Bank for such needs, if any, during the support period.
- xi. The Bidder support staff should be well-trained to effectively handle queries raised by the customers/employees of the Bank.
- xii. An updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.
- xiii. The data created during the Contract period will be the exclusive property of each Bank separately and the bidder shall not utilize/share with any third party/sell the same to any third party. The bidder shall comply with the Bank's security policy of Bank.

19. Right of Audit and Verification

- Both Banks, their internal and external auditors, statutory auditors, RBI, NABARD, CERT-In, and other regulatory/statutory authorities shall have the right to audit the Bidder's premises, processes, records, and systems related to services provided under this contract with consultation with the bidder.
- Bidder must provide unrestricted access to Bank-authorized personnel at any point during the contract period with reasonable advance notice.
- Banks reserve the right to verify claims made in the bid independently at any stage.

20. Fraud and Corrupt Practices

- I. The Bidder and their respective officers, employees, agents, and advisers shall observe the highest standard of ethics during the bidding Process. Notwithstanding anything to the contrary contained herein, the Bank shall reject an application without being liable in any manner whatsoever to the Bidder if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt/fraudulent/coercive/undesirable or restrictive practices in the bidding Process.
- II. Without prejudice to the rights of the Bank, if a Bidder is found by the Bank to have directly or indirectly or through an agent, engaged or indulged in any corrupt/fraudulent/coercive/undesirable or restrictive practices during the bidding process, such Bidder shall not be eligible to participate in any EOI/RFP issued by the Bank during a period of 2 (two) years from the date such Bidder is found by the Bank to have directly or indirectly or through an agent, engaged or indulged in any corrupt/ fraudulent/ coercive/ undesirable or

restrictive practices, as the case may be.

III. For this Clause, the following terms shall have the meaning hereinafter, respectively assigned to them:

(a) **“corrupt practice”** means

(i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the actions of any person connected with the bidding Process (for t h e avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the Bank who is or has been associated in any manner, directly or indirectly with the bidding process or the Letter of Authority or has dealt with matters concerning the Concession Agreement or arising there from, before or after the execution thereof, at any time before the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the Bank, shall be deemed to constitute influencing the actions of a person connected with the bidding Process); or

(ii) engaging in any manner whatsoever, whether during the bidding process or after the issue of the Letter of Authority or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Letter of Authority or the Agreement, who at any time has been or is a legal, financial or technical adviser of the Bank concerning any matter concerning the Project;

(b) **“Fraudulent practice”** means a misrepresentation or omission of facts suppression of facts or disclosure of incomplete facts, to influence the bidding Process;

(c) **“Coercive practice”** means impairing or harming or threatening to impair or harm, directly or indirectly, any person or property to influence any person’s participation or action in the bidding Process;

(d) **“Undesirable practice”** means (i) establishing contact with any person connected with or employed or engaged by the Bank with the objective of canvassing, lobbying, or in any manner influencing or attempting to influence the bidding process; or (ii) having a Conflict of Interest; and

(e) **“Restrictive practice”** means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the bidding Process.

21. Taxes and Duties

- I. The Vendor shall be liable to pay all corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India and the price Bid by the Vendor shall include all such taxes in the contract price.
- II. The rate (s) quoted should be inclusive of all Central / State Government taxes/duties, GST, and levies as per the Government notification in this regard, from time to time and shall be borne by the Vendor.
- III. Rate(s) payable to the Vendor as stated in the Contract shall be firm and not subject to adjustment during the performance of the Contract, irrespective of reasons whatsoever, including exchange rate fluctuations, or any upward revision in Custom duty. The Bidder will pass on to the Bank, all fiscal benefits arising out of reductions, if any, in Government levies viz. custom duty or the benefit of discounts if any announced in respect of the cost of the items for which orders have been placed during that period.

IV. All expenses, stamp duty, and other charges/ expenses in connection with the execution of the agreement as a result of this RFP process shall be borne by the Vendor.

22. Legal Relationship

Until execution of the formal contract, the bid document together with the Banks' notification of award and the Bidder's acceptance thereof shall constitute a binding contract between the Banks and the Successful Bidder.

23. Powers to Vary or Omit Work

- I. No alterations, amendments, omissions, additions, suspensions, or variations of the work (hereinafter referred to as variation) under the contract shall be made by the successful Bidder except as directed in writing by the Bank. The Bank shall have full powers, subject to the provision hereinafter contained, from time to time during the execution of the contract, by notice in writing to instruct the successful Bidder to make any variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable as though the said variations occurred in the contract documents. If any, suggested variations would, in the opinion of the finally selected Bidder, if carried out, prevent him from fulfilling any of his obligations under the contract, he shall notify the Bank thereof in writing with reasons for holding such opinion and Bank shall instruct the successful Bidder to make such other modified variation without prejudice to the contract. The finally selected Bidder shall carry out such variation and be bound by the same conditions as far as applicable, as though the said variations occurred in the contract documents. If the Bank confirms its instructions, the successful Bidder's obligations shall be modified to such an extent as may be mutually agreed if such variation is substantial and involves considerable extra cost. Any agreed difference in cost occasioned by such variation shall be added to or deducted from the actual cost arising as per the rate(s) finalized, as the case may be.
- II. In any case in which the successful Bidder has received instructions from the Bank as to the requirements for carrying out the altered or additional substituted work which either then or later on, will in the opinion of the finally selected Bidders, involve a claim for additional payments, such additional payments shall be mutually agreed in line with the terms and conditions of the order.
- III. If any change in the work is likely to result in a cost reduction, the parties shall agree in writing to the extent of change in contract price (rate), before the finally selected Bidder(s) proceeds with the change. In all the above cases, in the event of a disagreement as to the reasonableness of the said sum, the decision of the Bank shall prevail.

24. Waiver of Rights

Each Party agrees that any delay or omission on the part of the other Party to exercise any right, power or remedy under this RFP will not automatically operate as a waiver of such right, power or remedy or any other right, power or remedy and no waiver will be effective unless it is in writing and signed by the waiving Party.

Further the waiver or the single or partial exercise of any right, power or remedy by either Party hereunder on one occasion will not be construed as a bar to a waiver of **any successive or other right, power or remedy on any other occasion.**

25. Contract Amendments

No variation in or modification of the terms of the Contract shall be made, except by written amendment, signed by the parties.

26. Bank's Right to Accept Any Bid and to Reject Any or All Bids

- i. This RFP is not an offer to contract but rather is to be used to establish a common framework within which an agreement can be reached. Bidder shall warrant and put forth in writing that the deliverables and services proposed shall be performed, at the minimum, in accordance with all requirements specified herein in such a manner to achieve the overall intent and purpose described in this RFP.
- ii. The Bank reserves the right to accept or reject any Bid in part or in full or to cancel the bidding process and reject all Bids at any time before contract award, without incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Bank's action.

27. System Integration Testing & User Acceptance Testing

Service Provider should integrate the software with the existing systems as per requirement of the Bank and carry out thorough system integration testing. System integration testing will be followed by user acceptance testing, plan for which has to be submitted by Service Provider to the Bank. The UAT includes functional tests, resilience tests, benchmark comparisons, operational tests, load tests etc. Bank's staff / third Party vendor designated by the Bank will carry out the functional testing. This staff / third party vendor will need necessary on-site training for the purpose and should be provided by Service Provider. Service Provider should carry out other testing like resiliency/benchmarking/load etc. Service Provider should submit result log for all testing to the Bank.

On satisfactory completion of the aforementioned tests, the User Acceptance Test (UAT) letter will be issued to Service Provider by the competent authority.

28. Warranty and Annual Maintenance Contract

i. The selected Bidder shall support the solution during the period of warranty and AMC (if included in purchase order) as specified in Scope of work in this RFP from the date of acceptance of the Solution by both the banks.

ii. During the warranty and AMC period (if desired), Bidder will have to undertake comprehensive support of the Solution supplied by the Bidder and all new versions, releases, and updates for all standard software to be supplied to the Bank at no additional cost . During the support period, the Bidder shall maintain the Solution to comply with parameters defined for acceptance criteria and the Bidder shall be responsible for all costs relating to labour, spares, maintenance (preventive and corrective), compliance of security requirements and transport charges from and to the Site (s) in connection with the repair/ replacement of the Solution, which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified.

iii. During the support period (warranty and AMC, if desired), Service Provider shall ensure that services of professionally qualified personnel are available for providing comprehensive on-site maintenance of the Solution and its components as per the Bank's requirements. Comprehensive maintenance shall include, among other things, day-to-day maintenance of the Solution as per the Bank's policy, reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/mal functioning, arranging and configuring facility as per the requirements of the Bank, fine tuning, system monitoring, log maintenance, etc. The Bidder shall provide services of an expert engineer at Bank's locations wherever required, whenever it is essential. In case of failure of Solution, Bidder shall ensure that Solution is made operational to the full satisfaction of the Bank within the given timelines.

iv. Warranty/ AMC (if opted) for the system software/ off-the shelf software will be provided to the Bank as per the general conditions of sale of such software.

v. Support (Warranty/ AMC, if opted) would be on-site and comprehensive in nature and must have back to back support from the OEM/Service Provider. Service Provider will warrant products against defects arising out of faulty design etc. during the specified support period.

vi. In the event of system breakdown or failures at any stage, protection available, which would include the following, shall be specified.

- (a) Diagnostics for identification of systems failures
- (b) Protection of data/ Configuration
- (c) Recovery/ restart facility
- (d) Backup of system software/ Configuration

vii. Prompt support shall be made available as desired in this RFP during the support period at the locations as and when required by the Bank.

viii. The Bidder shall be agreeable for on-call/on-site support during peak weeks (last and first week of each month) and at the time of switching over from DC to DR and vice versa. No extra charge shall be paid by the Bank for such needs, if any, during the support period.

ix. Bidder support staff should be well trained to effectively handle queries raised by the customers/employees of the Bank.

x. Updated escalation matrix shall be made available to the Bank once in each quarter and each time the matrix gets changed.

29. Non-Sharing of Resources

All dedicated resources including premises, personnel, and technology for both Banks, when are free and are not in use, will be left to remain idle and the bidder shall not use these for any other process due to security reasons.

30. Validity of Agreement

The Agreement/ SLA will be valid for the period of the contract. The Bank reserves the right to terminate the Agreement as per the terms of the RFP.

During the shifting of the services to the new bidder, the selected bidder shall provide necessary help for the smooth switch over, and necessary information support to both Bank's staff and/or Bank's-appointed third party, for running the EFRM operations without any additional cost, thus ensuring continuity of service to Bank's customers. During the transition the price paid to vendor will be same as initially contracted even if the term runs beyond contract period.

31. DELAY IN THE VENDOR'S PERFORMANCE:

I. Services shall be made available by the Vendor within the timelines prescribed in this document.

II. If at any time during the performance of the Contract, the Vendor should encounter conditions impeding timely delivery and performance of Services, the Vendor shall promptly notify the Bank in writing of the fact of the delay, its likely duration, and cause(s). As soon as practicable after receipt of the Vendor's notice, the Bank shall evaluate the situation and may, at its discretion, extend the Vendor's time for performance, in which case, the extension shall be ratified by the parties by amendment of the Contract.

III. Any delay in performing the obligation/ defect in performance by the Vendor may result in the

imposition of penalty, liquidated damages, invocation of Performance Bank Guarantee, and/or termination of the contract (as laid down elsewhere in this RFP document)

32. VENDOR'S OBLIGATIONS:

I. The Vendor is responsible for and obliged to conduct all contracted activities in accordance with the contract using state-of-the-art methods and economic principles and exercising all means available to achieve the performance specified in the Contract.

II. The Vendor is obliged to work closely with the Bank's staff, act within its own authority abide by directives issued by the Bank from time to time, and complete implementation activities.

III. The Vendor will abide by the job safety measures prevalent in India and will free the Bank from all demands or responsibilities arising from accidents or loss of life, the cause of which is the Vendor's negligence. The Vendor will pay all indemnities arising from such incidents and will not hold the Bank responsible or obligated.

IV. The Vendor is responsible for managing the activities of its personnel or sub-contracted personnel (where permitted) and will hold itself responsible for any misdemeanours.

V. The Vendor shall treat as confidential all data and information about Banks, obtained in the process of executing its responsibilities, in strict confidence and will not reveal such information to any other party without prior written approval of the Bank as explained under 'Non-Disclosure Agreement' in [Annexure-VI](#) of this document.

VI. Bidders need to exchange mail (through the Bank's Domain), and store data/files on a laptop/desktop. There should be a provision for regular backups of the laptop/desktop/servers. Back-up should be stored/archived as per regulatory guidelines and access management to the same must be restricted. Bank / Regulatory authorities may call for such communication/data for compliance purposes.

VII. During the contract period organic as well as inorganic growth, the volume and number of transactions will not make any impact of price of solution / commercial.

33. TECHNICAL DOCUMENTATION:

I. The vendor shall provide documents related to review records/ Test Bug Reports/ Root Cause Analysis Reports, a list of all Product components, Data Dictionary, a list of all dependent/external modules, and a list of all documents relating to traceability of service level failure, within mutually agreed TAT as and when required by the Bank.

The Vendor shall also provide the MIS reports as per requirements of the Bank. Any level/ version changes and/or clarification corrections or modifications in the above-mentioned documentation should be supplied by the Vendor to the Bank, free of cost promptly

**SECTION – III: BROAD SCOPE OF WORK – ENTERPRISE FRAUD RISK
MANAGEMENT SOLUTION**

1. About the Project

The purpose of this Joint Request for Proposal is to procure an Enterprise Fraud Risk Management (EFRM) Solution that will be installed, implemented, managed, and maintained for Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB) as two separate, independent deployments under a single vendor contract. The quality, reliability, scalability, and regulatory compliance of the EFRMS are of prime importance for the risk mitigation and fraud prevention objectives of both Banks.

2. Project Objectives

Both Banks are offering various digital and physical delivery channels to their customers. It is therefore imperative that the EFRM Solution deployed for each Bank is capable of:

- Supporting the prevention, detection, analytics, and management of frauds across user profiles, accounts, products, processes, and channels in real-time, independently for each Bank.
- Monitoring, analysing user activity, behaviour, and trends at the application level to observe what transpires inside and across customer accounts using all banking channels.
- Analysing behaviour among related users, accounts, customer profiles, or other entities to identify organised criminal activity, fraud rings, money mule networks, corruption, or misuse.
- Providing highly complex algorithms, sophisticated system architecture and design, AI/ML models for predictive analysis, and response times measured in milliseconds.
- Detecting, investigating, and preventing fraud across all delivery channels: Online/Mobile Banking, ATM, UPI, AEPS, CBS Branch Transactions, IMPS, NEFT/RTGS, BBPS, and any new channels launched during the contract period.
- Reducing fraud losses by improving fraud detection accuracy while significantly reducing false positives and false negatives.
- Enhancing regulatory compliance with all applicable RBI, NABARD, DFS, CERT-In, and DPDP Act requirements.
- Improving operational efficiency through streamlined fraud risk management processes and automated regulatory reporting.
- Ensuring real-time integration with I4C/NCRP cybercrime complaint systems and automated T+0 debit freeze and push-back functionality.
- Providing NABARD-specific fraud returns and supervisory reports (mandatory for both Banks as RRBs under NABARD supervision).

3. Scope of Work – General Requirements

3.1 The EFRM solution should have harmless cutting-edge AI and machine learning models to enable sophisticated risk based scoring, proactive fraud prevention, real time detection. The solution will incorporate specialized mule and scam detection models, advanced network and graph analytics for identifying complex fraud patterns. In addition, the EFRM solution will provide interactive rule simulation tools, intuitive dashboards, for insightful monitoring, and end-to-end workflow automation to streamline investigative and operational process.

The Successful Bidder will provide an enterprise-wide EFRM Solution for both Banks independently, incorporating comprehensive controls for identifying suspicious transactional behaviour through rules, preventive and detective controls, customer alert / capturing response mechanisms, and related capabilities across all integrated source systems and new initiatives launched during the contract period. The scope of work includes the following:

1. Standard off the shelf Modules for Enterprise wide Fraud risk management solution including but not limited to Case Manager, Scenario / rule manager, Decision Engine, Rule simulator, Dash boarding platform, Enterprise reporting module, Data sandbox, workflow management etc. customized as per the requirement of the Bank.
2. Development of the AI/ML models and advanced analytics module and related technologies

3. Supply of Manpower post Go-live for continuous development and enhancement.

3.2 The Successful Bidder will provide Term Enterprise Licenses and ATS for the implementation period + 5 years for both Banks independently. The proposed licensing model may be based on a secure multi-tenant architecture supporting both Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB) under a common software platform, provided that complete logical segregation of data, users, configurations, rules, workflows, reports, audit trails, and administrative controls is maintained between the two Banks.

The license shall entitle each Bank to independently use, configure, administer, and operate its respective EFRMS environment without any dependency on the other Bank.

3.3 Scope includes implementation at Primary Data Centre (including Test/Development/Training environments) and Disaster Recovery (DR) Site for each Bank independently. In case either Bank's DC and/or DR relocates during the contract period, the Bidder will support relocation at no additional cost.

3.4 The proposed EFRM Solution must be integrated with the following delivery channels and applications of each Bank in both Real-Time & Near Real-Time/Batch mode in Preventive (Deny) and Detective (Alert) mode for Financial Transactions (Inward & Outward), Non-Financial Transactions, and Authentication purposes:

3.4.1 PHASE 1 – Installation of databases and application Software at Bank's DC/ DR infrastructure hosted at primary data centre in Mumbai and at the Bank's DR premises in Hyderabad / Mumbai or/and any premises decided by the Bank along with testing of all the functionalities specified in the RFP and integration of all the channels specified in the scope with the solution in UAT environment. (within 30 days from PO date)

3.4.2 PHASE 2 - Priority Implementation (within 90 days from PO)

S.No.	Channel / System	Mode	Direction	Notes
1	UPI (Unified Payments Interface)	Real-Time	Inward & Outward	
2	Core Banking Solution	Real-Time	Inward & Outward	Mandatory. Includes: Internal Accounts, Staff Accounts, Deposit/Loan Accounts, Dormant Accounts, New Accounts, Money Mules, CTS, NACH, PFMS, Open API, etc. Near Real-Time ≤ 3 seconds.
3	Mobile Banking	Real-Time	All Transactions	Application
4	Internet Banking	Real-Time	All Transactions	
5	Debit Card (ATM Switch)	Real-Time	Outward	Including POS and E-Commerce card transactions

S.No.	Channel / System	Mode	Direction	Notes
6	IMPS	Real-Time	Inward & Outward	
7	AEPS (Aadhaar Enabled Payment System)	Real-Time	All Transactions	Including BC-channel transactions
8	NEFT & RTGS	Real-Time	Inward & Outward	
9	FRI/MNRL	Real-Time	Inward & Outward	
10	Deployment of Core analytics: <ul style="list-style-type: none"> Case Management Rule Management Reporting & Dashboard Rule simulator, Test Environment, and Sandbox Decision Engine User Access Management Alert Management 			
11	Development & Customization of Advanced Analytics <ul style="list-style-type: none"> AI-Based transaction scoring model Scam detection Mule detection Anomaly detection Network / Link & Graph analysis 			
12	AML solution			

Note: All the delivery Channels have to be integrated strictly in Real Time/ Preventive (deny) mode. However, the proposed solution should Prevent (deny) and Monitor (alert) frauds in both real-time and near real-time (response time of less than 3 second) mode at an Enterprise Level. Few Rules may be configured in Near Real Time (NRT) mode and also in Batch mode as per the Bank's requirement. Real Time and Near Real Time (NRT) are defined as response time of less than 100 milliseconds and 3 seconds respectively.

3.4.3 PHASE 3 – Extended Integration (within 120 days from PO date)

S.No.	Channel / System	Mode	Notes
1	SMS Gateway	Real-Time	For 2FA, OTP, TOTP, risk-based authentication triggers, and alert SMS
2	Email Gateway	Real- Time	For 2FA and risk-based email alerts
3	IVRS	Detective/Alert	Outbound
4	BBPS (Bharat Bill Payment System)	Real-Time Preventive	Inward & Outward
5	Behavioural Biometric Application	Real-Time	Vendor provides SDK for Android, iOS, and JavaScript (Internet Banking). Full integration with Device Intelligence module.

S.No.	Channel / System	Mode	Notes
6	<ul style="list-style-type: none"> Payment Gateway / Payment Aggregators, Government Business Transactions, PFMS NPCI EFRMS (National Payments Corporation of India EFRM System feeds) Any additional channels deployed by either Bank during the contract period External Threat Intelligence Feeds: Neustar, Maxmind, Lexis Nexis, Group-IB, RSA, I4C Suspect Registry, CFR, CIBIL, CRILC, ECGC, DIP, and others as required 	NRT/Real-Time	
7	<ul style="list-style-type: none"> HRMS 		

3.5 For Customer Outreach, the EFRMS must be integrated with: Call Centre & IVRS; SMS Gateway (for 2FA and risk-based authentication); Email Gateway (for risk-based scenarios); Step-Up Authentication Application; and Behavioural Biometric Solution.

3.6 The EFRMS must accept and provide feeds to/from: KYC/AML Application; Early Warning Signals (EWS); DoT FRI/MNRL Data; I4C/NCRP; OSM Application (Off-Site Monitoring); External threat intelligence feeds; Any other system as directed by the respective Bank.

4. Performance Requirements

Parameter	Banks Requirement	Joint Minimum Standard
Peak TPS	1,500 TPS (scalable to 10,000)	1,000 TPS for UPGB instance; 500 TPS for GGB instance. Separate hardware sizing per Bank.
Real-Time Response Time	≤ 100 milliseconds	≤ 100 milliseconds for ALL channels at ALL times. Zero tolerance for breach.
Near Real-Time (CBS/NRT)	≤ 3 seconds	≤ 3 seconds
System Uptime	≥99.90% per quarter	≥99.90% per quarter (24×7×365) measured independently per Bank.
RTO (Recovery Time Objective)	≤ 120 minutes	≤ 120 minutes (adopted from UPGB's stricter standard). Mandatory for both Banks.

Parameter	Banks Requirement	Joint Minimum Standard
RPO (Recovery Point Objective)	≤ 10 minutes	≤ 10 minutes. Real-time replication DC to DR.
CPU/Memory at Peak Load	≤70% utilisation	≤70% at peak. If exceeded 5 times/day or 10 times/week, Bidder must fine-tune at no extra cost.
Concurrent User Sessions	150 minimum	Minimum 150 simultaneous sessions without performance degradation.
DR Drill Frequency	Quarterly	Quarterly, independently for each Bank. Bidder to demonstrate DR drill before Phase 2 Go-Live.

5. Finacle CBS Integration (Mandatory)

- Out-of-the-box integration with Finacle Core Banking System without dependency on Infosys/CBS vendor engagement.
- New versions and patches of Finacle must be supported throughout the contract period at no additional cost.
- EFRM Solution must NOT adversely impact performance of Finacle CBS at either Bank.
- All CBS customisations required for integration are the sole responsibility of the Bidder at no extra cost.
- Intelligence derived from CBS must enrich risk scoring for all alternate delivery channels in real-time.
- Solution should have demonstrable Out-of-Box integration capability with Finacle.

6. Data Segregation and Multi-Bank Architecture

▲ IMPORTANT: Complete segregation of data between Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB) shall be mandatory. Under no circumstances shall any transaction, customer, behavioural, case management, alert, investigation, reporting, or operational data of one Bank be accessible to the other Bank.

- The proposed EFRMS shall support a secure multi-tenant architecture, enabling UPGB and GGB to operate as completely independent tenants under a common software platform and licensing framework.
- Each Bank shall have dedicated logical segregation of databases/schemas, application configurations, fraud rules, workflows, case management repositories, reports, dashboards, audit trails, and user access controls.
- Separate administrative control shall be provided to each Bank. Users and administrators of one Bank shall not be able to view, access, modify, or administer any data, configuration, alerts, or cases belonging to the other Bank.
- Cross-bank data access at any layer, including application, database, API, network, reporting, backup, or operational support layer, shall be strictly prohibited.
- The Bidder shall ensure that all data generated by each Bank remains logically isolated throughout its lifecycle, including processing, storage, archival, backup, restoration, and disaster recovery operations.
- The Bidder shall conduct an independent security assessment of the multi-tenant segregation architecture and submit a certification confirming effective tenant isolation before Phase-2 Go-Live.

- Personnel deployed for UPGB implementation and support shall not be granted access to GGB data and systems, and vice versa, except with explicit written authorization from the concerned Bank and through auditable access controls.
- The solution shall demonstrate compliance with RBI, NABARD, and applicable cybersecurity and data protection requirements relating to tenant isolation and data confidentiality.

7. Detailed Functional Requirements

7.1 Core Fraud Detection Engine

- Advanced rule/scenario-based detection with no limit on the number of rules, scenarios, or policies that can be configured.
- AI/ML predictive scoring: self-learning, self-calibrating, explainable AI (XAI) using SHAP or LIME techniques.
- Risk Score transparency: exact reasoning for any risk score available to Bank analysts in the investigation UI.
- 360° customer view: cross-channel financial and non-financial transactions, CBS data, digital behaviour, device data.
- Cross-channel fraud correlation in real-time using CIF (Customer Identification Number) as the universal identifier across all integrated channels.
- Network analytics: social network analysis, entity link analysis, hub-and-spoke mule ring detection.
- Risk score scale: 1–1000 with configurable base scores and push-up/push-down factors.
- Support for Preventive (Deny), Detective (Alert), and Monitor (Shadow) modes per scenario.
- Whitelisting based on Customer/Account/Scheme-code/Transaction Type/Channel or combinations, readily available in the solution.
- EFRM may call the APIs and the other files formats which are generated from the CBS. The customizations required for the consumption of the APIs and the files, needs to be undertaken by the EFRM bidder. CBS can also call the APIs of EFRM, but with respect to the workflow of CBS, the APIs in EFRM may require customizations to suit the workflows and data structure of CBS. Such customizations to the EFRM APIs to be done by the bidder.
- Solution should provide complete evidence for why a transaction was declined/hold by the fraud management system.
- Solution should have a capability to whitelist a Customer/Card/Account for a user defined period for not triggering the alerts, but evidence data should be available within the solution.
- The various source channels may share Account number/Card Number/ Masked Aadhar number/Mobile number/CIF etc. in the financial/non-financial messages. However, the proposed EFRM Solution must carry out the fraud prevention across all transaction channels strictly based on a common unique identifier. For example: Customer Identification Number (CIF no) etc.
- Proposed solution should monitor, alert, decline, hold and challenge transactions in Real-time.
- The proposed solution should allow to configure various business policies like approve/decline/challenge/hold/block/freeze on transactions/accounts/channels based on the fraud risk score.
- Composition of risk score should be transparent to Bank (i.e. the exact reason for a high core will be available to Bank staff to enable accurate decision-making).
- Proposed system should support setting limits on the number of Internet Banking/Mobile banking beneficiaries that may be added in a day per account and provide alerts based on a threshold number of beneficiaries.
- Proposed solution should be able to blacklist various entities such as customer IDs, accounts, Registered mobile number, IPs etc.
- Solution should support all types of browser and operating systems environment on all devices e. g. Personal Computers/ Laptops/Smart phones/ TABS/ other devices.
- Proposed solution should be able to integrate with Bank's existing and future authentication process (SMS/OTP/MFA/Step Up Authentication)/application for stronger authentication. The solution should be capable of complying with the RBI Authentication Direction 2025.

- Bank will implement risk-based authentication solution for internet banking, mobile banking, e-commerce payments and other delivery channels of the Bank.
- The proposed solution should have the facility wherein alerts can be parameterized and monitored in terms of various applicable parameters. Such parameters, as applicable could be: transaction velocity (e.g., fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries, etc.) in a short period, more so in the accounts of customers who've never used mobile app/ internet banking/ card ever (depending upon the type of payment channel), high risk merchant category codes (MCC) parameters, counterfeit card parameters (String of Invalid CVV/ PINs indicates an account generation attack), new account parameters (excessive activity on a new account), time zones, geo-locations, IP address origin (in respect of unusual patterns, prohibited zones/ rogue IPs), behavioral biometrics, transaction origination from point of compromise, transactions to mobile wallets/ mobile numbers/ VPAs on whom vishing fraud or other types of fraud is/are registered/ recorded, declined transactions, transactions with no approval code, etc.
- The proposed solution should also be able to identify and prevent fraudulent transactions which are linked to non-monetary transaction such as ATM pin change, address/mobile no. change request, balance enquiry, beneficiary details addition/modification etc.
- The proposed solution should support real-time data ingestion from multiple channels and applications to maintain data freshness.
- Assign a dynamic risk score to each transaction based on real-time analytics and historical patterns.
- Enable risk-based prioritization to address the most critical cases first.
- The proposed solution should support cross-channel fraud monitoring and prevention in Real Time at an Enterprise level as opposed to silo based approach.
- Machine learning models should be incorporated to fine-tune risk scores continuously. AI/ML capabilities of the solution should be clearly demonstrated by the selected bidder.
- Solution should be able to add/remove customer/account into various watch lists based on case feedback.
- The proposed solution should allow end user to configure custom dashboard and reports based on transaction parameters, profiles, cases, customer/account attributes.
- Proposed Solution should have ability to manually assign alerts to users.
- System should support provision to block a channel facility (for e.g. Mobile Banking/Internet Banking/UPI/ECOM/POS etc.) with respect to any entity.
- The solution must be able to use the inputs from the online fraud monitoring services (anti-Phishing, anti- Pharming, anti- Trojans, anti-Rogue etc.) such as suspected IPs, suspected locations, compromised accounts, Mule account details used by various Trojan families, dummy data fed to fraud sites etc. and other inputs provided by the bank and third parties.
- The proposed solution should automatically trigger alerts through Mail/SMS to concerned stake holders if there is no Heartbeat or Response from the EFRMS.
- Proposed solution should have the capability to perform specific transaction monitoring and fraud detection/non-compliance scenarios for new accounts (say accounts of vintage less than 6 months).
- The solution should have proven integration capabilities with the CBS and bidder should ensure that the EFRM solution does not have a performance impact on the CBS or any other channel.

7.2. Customer Profiling:

Customer profiling refers to creation of profiles for each customer where at least one transaction pertaining to the customer has been routed through EFRMS, the customer profiling should be dynamic in nature covering Transaction, Behavioral and Demographic details of the customers. Customer profile should be updated dynamically based on the transactions performed by customer on real time basis which should include but not limited to the following indicative parameters

- a) **Transactional Data:** Purchase history, payment methods, transaction frequency, amounts, locations, and time of day etc.
- b) **Demographic Data:** Age, gender, location, occupation, income etc.

- c) **Behavioural Data:** Website browsing patterns, application usage, login history etc.
- d) **Device Data:** IP addresses, device IDs, operating systems, browser information, History of devices used by the customer, Favourite UPI handles etc.
 - Solution should have the capability to use various parameters such as transaction velocity, geo-locations, latitude and longitude, IP address origin for triggering the alert after configuration. Solution should monitor and detect login, pre-login and post login frauds. It should support advanced IP Geo location capability to detect IP country, IP City, Proxy IP and zone hopping.
 - Solution should have capability to build and re-factor dynamic e-banking user behavior profiles including but not limited to preferred country, preferred city, preferred IP, preferred ISP, preferred device, preferred payee etc.
 - Solution should monitor Average Daily/Weekly/Monthly Funds Transfer amount / frequency by payee / biller and also preferred transaction hours.
 - Solution should have the capabilities to correlate transaction with customer profile (such as location, registration of mobile devices, illiterate check, usage of Digital channels etc.) to identify potential fraud.
 - Solution should support out of the box behavior profiles including but not limited to Card holder profiles, Preferred ATM machines, Preferred Merchants, Preferred Merchant Category Codes, preferred Country /City, Preferred Time Period, Preferred Transaction hour for ATM, POS, E-Commerce, Preferred Currency for purchase-Average Daily/ Weekly/ Monthly/ Quarterly/ Season based transaction amount by channel (for domestic and international transactions), Average daily/Weekly/Monthly/Quarterly/Season based transaction frequency by channel (for domestic and international transactions).
 - Solution should support to set threshold limit with specified time periods for all cards that have not been used for international transactions in the past.
 - Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.
 - System should look for anomalous activity in customer accounts. It should detect behavior associated with a fraudulent transaction. Updated customer contact information is critical for quickly verifying the legitimacy of transactions or stopping fraud.
 - In addition to the above the Solution should also have the capabilities to accommodate third party data if any which will be provided by the Bank.
 - The customer profiling should be available at both Micro level and Macro level wherein Micro level meaning the individual customer profile and the Macro level being the entire subset to which the customer belongs and whether customer profile commensurate with other peers present in the same demographics.
 - Creation of rules based on few attributes or rules based only on Transactional data /Demographical Data/behavioral data in silo basis is not considered as customer profiling.
 - Customer profiling should be a default part of the Risk and decisioning system of the solution and there by any decision take by the rule engine should factor the customer profiling without any dependency on the rules.
 - In case of customers where profile is created and there are no transactions for a minimum period of 1 year then such profiles to be maintained separately.
 - The solution should have an effective design for limiting the use of Hardware that is required for creation and maintenance of customer profiles.

7.3 Scenario Authoring Tool (Rule Engine)

- GUI-based scenario/rule authoring tool with full Maker-Checker workflow integrated with Active Directory (AD)/HRMS.
- Scenario definition using: Transactional Data, Entity Master Data, Watchlist/Blacklist data, Device intelligence data, and any other data source imported into the system.
- Out-of-Box mathematical functions: min, max, avg, sum, count, etc.
- Out-of-Box logical functions: equal to, not equal to, greater than, less than, between, etc.
- Out-of-Box string functions: matches, contains, starts with, ends with, etc.

- Deployment of scenarios in Silent Mode (monitoring only) or Decision Mode (preventive).
- Default configuration for feedback-based false positive suppression for a configurable duration.
- Capability to reset trackers for specific events upon case/alert closure.
- 500 rule customisations per year included under ATS at no additional cost. RBI/NABARD-mandated rule updates are free of cost throughout the contract period.

7.4 Channel-Specific Fraud Scenarios (Minimum Out-of-Box)

7.4.1 UPI and QR Transaction Monitoring

- Profile/behaviour-based scenario on UPI transactions.
- Transaction history-based scenario with velocity checks.
- Risk score-based blocking/alerting.
- SIM Swap detection and alerting.
- Device Cloning / Device Change monitoring.
- Fake Merchant detection using MCC code analysis.
- P2P and P2M transaction anomaly detection.
- Frequent linked bank account changes.
- First-time high-value UPI transaction.
- UPI transaction from unusual geolocation or high-risk PIN code.
- Or any other scenarios as per bank's requirement

7.4.2 AEPS Transaction Monitoring

- Profile/behaviour-based scenario.
- Transaction history and risk score based scenario.
- Repeated fingerprint mismatch failures.
- Transactions from suspicious BC agents.
- AEPS transactions from multiple locations in a short duration.
- Transactions to/from blacklisted entities.
- Transaction volume and frequency based anomaly.
- Unusual time-of-day AEPS transactions.
- Or any other scenarios as per bank's requirement

7.4.3 IMPS Monitoring

- Profile/behaviour-based scenario.
- First-time IMPS transaction with unusually large amount.
- Single mobile device initiating IMPS transactions for multiple accounts.
- Velocity-based IMPS monitoring.
- IMPS to high-risk accounts or blacklisted beneficiaries.
- Risk score based scenario.
- Transaction number, frequency and volume based scenario.
- Or any other scenarios as per bank's requirement.

7.4.4 Internet/Mobile Banking Monitoring

- Unusual login patterns (time, device, location, IP anomalies).
- Impossible travel detection (login from geographically distant locations in short timeframe).
- OTP abuse – multiple OTP requests.
- New beneficiary addition followed by immediate high-value transfer.

- Concurrent session anomaly.
- Password change followed by immediate high-value transaction.
- Fund transfers by different modes (RTGS/NEFT/IMPS etc).
- Or any other scenarios as per bank's requirement.

7.4.5 ATM/Debit Card Monitoring

- Card-not-present fraud detection.
- Counterfeit card pattern detection (string of invalid CVV/PIN attempts).
- Multiple ATM withdrawals in multiple locations in short timeframe.
- Cross-geography ATM withdrawal patterns.
- High-value POS transaction anomaly.
- Card skimming detection patterns.
- Profile/behaviour based scenario.
- Transaction history based scenario.
- Risk score based scenario.
- Or any other scenarios as per bank's requirement

7.4.6 CBS / Branch Transaction Monitoring

- New account with excessive activity.
- Internal account monitoring – entries not linked to customer transactions.
- Staff account monitoring – unusual activity by bank staff accounts.
- Dormant account sudden activation with high-value transactions.
- Unusual cash deposits/withdrawals patterns.
- CTS cheque fraud detection.
- NACH mandate abuse detection.
- Or any other scenarios as per bank's requirement.

7.4.7 Money Mule / Cyber Fraud Detection (Mandatory)

- Multiple inbound transactions from unrelated sources.
- Suspicious inbound transactions with immediate outward transfer.
- Large inbound transfers from unknown sources followed by immediate withdrawal.
- Circular transactions (Round-tripping and layering detection).
- Frequent small inbound and outbound transfers (structuring/smurfing).
- Classification: First-level mules, second-level/layered mules, synthetic identity mules, unwitting vs. complicit mules.
- Network analytics: graph-based mule ring identification and hub-and-spoke structure detection.
- Separate investigation queue in CMS for suspected mule accounts.
- Integration with DoT's FRI/MNRL for mule account detection.
- Integration with I4C Suspect Registry for mule account data exchange.
- Automated STR generation for FIU-IND filing for confirmed mule accounts.
- Or any other scenarios as per bank's requirement.

7.4.8 Illiterate / Vulnerable Customer Enhanced Monitoring (Mandatory for Both RRBs)

- Solution must flag accounts where the customer is marked as illiterate or vulnerable in CBS (e.g., thumb-impression authentication).

- Enhanced monitoring rules for: high-value transactions from illiterate accounts; sudden digital channel activation; unusual beneficiary addition; out-of-profile transactions; transactions outside normal geography.
- Risk scoring must factor in customer literacy/vulnerability status derived from CBS.
- Separate alert queue and escalation for transactions involving vulnerable customers.

NOTE: This is a mandatory requirement. Both UPGB and GGB serve large rural populations with significant proportions of illiterate and semi-literate account holders. Failure to include this capability is grounds for disqualification.

7.5 AI/ML Governance Framework (Mandatory)

- AI/ML Governance Framework aligned with RBI FREE-AI guidelines and ISO/IEC 42001 (Artificial Intelligence Management System standard).
- Centralised Model Risk Register: capturing model type, purpose, data inputs, ownership, deployment timelines, validation dates, and risk classification for all models.
- Independent model validation prior to deployment and at least semi-annually thereafter. Validation reports covering performance evaluation, back-testing, and scenario testing must be shared with respective Banks upon request.
- End-to-end model lifecycle management: development → testing → deployment → version control → periodic review → decommissioning.
- Bias monitoring framework to detect and mitigate discriminatory outcomes in fraud scoring – especially for rural demographics and vulnerable customer segments. Annual bias audit report required.
- Explainable AI (XAI): SHAP or LIME techniques for all complex models. Bank analysts must understand why a specific transaction was flagged.
- Model performance reports for last 3 years or versions to be submitted with Technical Bid.
- Auto-closure of low-risk alerts based on AI/ML risk scores – threshold configurable independently by each Bank.
- Primary scanning of generated alerts using AI/ML to reduce manual effort for fraud analysts.
- Any material change to deployed models requires prior written approval of the respective Bank.

7.6 NABARD Regulatory Reporting (Mandatory for Both Banks as RRBs)

△ IMPORTANT: NABARD regulatory reporting is mandatory for both Banks as they are Regional Rural Banks under NABARD supervision. Any solution failing to support this is disqualified.

- Automated generation of NABARD-prescribed fraud returns and RRB-specific supervisory reports.
- Configurable templates for NABARD reporting formats – updatable without requiring redevelopment.
- Auto-scheduling, auto-generation, and export in NABARD-acceptable formats (XLS, CSV, PDF, API).
- Complete data accuracy with audit trails and drill-down capability for regulatory verification.
- Centralised historical data, reports, logs, and evidence accessible for NABARD inspections.
- Free system updates when NABARD revises reporting formats during the contract period.
- Support for RBI cyber incident reports in prescribed format for reporting to RBI C-SOC and CERT-In.
- Automated generation and submission-ready format for all returns required by RBI/NABARD.

7.7 I4C / NCRP Integration (Mandatory)

- Real-time API-based integration (TLS 1.3, upgradeable) with: NCRP (cybercrime.gov.in), CFCFRMS/1930 helpline, I4C Suspect Registry, and Digital Intelligence Platform (DIP).

- Automated ingestion of fraud complaints from I4C with real-time parsing, alert generation, and case creation within the EFRMS.
- T+0 debit freeze / lien marking: rule-based automated workflows with CBS integration and Maker-Checker controls. Full audit trail of all freeze/lien actions.
- Real-time / near real-time push-back of account/action status to I4C with acknowledgement tracking, retry mechanism, and exception handling.
- Integration with I4C Suspect Registry for both ingestion of suspect data and reporting of confirmed fraud data.
- Automated generation of cyber incident reports in RBI-prescribed format for reporting to RBI C-SOC and CERT-In within mandated timelines.
- Dashboards and MIS for monitoring complaint-to-action timelines, SLA compliance, and exceptions.
- All I4C/NCRP activities must be fully auditable with immutable logs.
- Bidder shall ensure defined SLA adherence for I4C complaint processing and provide dashboards for monitoring.

7.8 Watch List Management

- Support for whitelist and blacklist management for various entities: CFR (Central Fraud Registry), ECGC, I4C Suspect Registry, MNRL, FRI, and others.
- Bulk upload of watchlist files via CSV/API (TLS 1.3).
- Manual entity marking into watchlists from within the investigation workflow.
- Automated updates from I4C/NCRP and DoT FRI/MNRL databases.
- Watchlist checks across all integrated channels in real-time.

7.9 Case Management System & MIS (CMS)

- Provide self-service, low-code/no-code BI platforms for users across business, investigative, administrative, executive roles, fraud analysts, operations, and management with rich visualization options (charts, heat maps, KPIs)
- 150 simultaneous concurrent user sessions minimum (independent per Bank) without performance degradation.
- 360° Customer View: Customer parameters (Name, DOB, PAN, Aadhaar, Address, Email, Mobile, Customer Segment, Income, Literacy Status, etc.); Account parameters (Account Type, Scheme Code, Status, Open Date, Balance); Staff parameters (Staff ID, Designation, Department, Joining Date); Transaction history; Case/Alert history.
- Transactional Link Analysis: cross-channel CBS Funds Transfer data-based account linkages shown via UI. Multi-level drill-down.
- Case creation within 3 seconds of EFRM system's transaction response.
- Deliver diverse visualizations (charts, heat maps, KPIs) and support multi-dimensional slicing and drill through capabilities.
- Build role based dashboards optimized for fraud analysts, supervisors, call centres, business analysts and executives.
- Include performance management dashboards tracking analysts productivity, model accuracy, rule effectiveness and system performance.
- Support ad-hoc investigation reporting, historical case analytics, and operational MIS reports.
- Provide audit-ready documentation and secure historical report repositories.
- Configurable case workflows per case type. Default: Case creation → assignment → investigation → resolution → closure.
- Provide end-to-end workflow management from alert generation to case closure with full audit trails and dynamic role-based access.

- Support maker-check authorizations on critical actions, change approvals, and emergency workflows.
- Auto-routing with Round-Robin, Load-Balanced, and Manual assignment options.
- N-level case escalation with auto-escalation on SLA breach.
- PCI-DSS compliant card data masking in CMS UI.
- RBI fraud categorisation-based case classification for regulatory reporting.
- Alert closure review mechanism: ability to re-open closed alerts for supervisor review.
- Email integration: all changes in case/alert status communicated to assigned team.
- Bulk processing: change state, reassignment, add comments, modify values in batch.
- Evidence field capturing transaction synopsis that triggered the alert.
- Attachment capability: documents, screenshots, evidence files attachable to cases.
- Ability to assign cases/alerts to specific investigators.
- Saved and shared search filters accessible team-wide.
- Parent case view: all alerts under a single customer/account visible under one parent case.
- Automated STR generation workflow for FIU-IND for mule account cases.
- Ability to mark alerts as Fraudulent/Non-Fraudulent with sub-classifications.
- Minimum 9 months of live case data accessible online in CMS.

7.10 Device Intelligence and Behavioural Biometrics (Mandatory)

- Native or tightly integrated Device Intelligence and Behavioural Biometrics for all digital channels (Mobile Banking, Internet Banking, UPI/API transactions).

Behavioural Biometrics Parameters:

- Digital behavioural patterns: mouse activity, keyboard dynamics, touchscreen swipe patterns, mobile device movement.
- Presence of Remote Access Tools (RAT) and malware.
- Bot detection mechanisms.
- User interaction nature and timing assessment for risk scoring.
- Data entry pattern analysis.

IP Intelligence:

- TOR IP detection.
- Malicious IP detection.
- Proxy and VPN IP detection.
- Blacklisted IP detection.

Device Intelligence:

- App cloning and app tampering detection.
- Emulator detection.
- Rooted/jailbroken device detection.
- Mock GPS/location spoofing detection.
- Remote session / Adaptive Call detection.
- SIM swap and SIM change frequency monitoring.
- Debuggable app detection.

Browser-Level Anomalies:

- Incognito mode detection.
- Ad blocker detection.
- Anonymisation attempts.
- True User Agent identification.
- Timezone manipulation detection.

SDK Requirements:

- Mobile SDKs for Android and iOS platforms.
- JavaScript components for Internet Banking portal integration.
- Vendor must disclose: OEM/Provider Name and details, SDK functional capabilities, performance impact/latency, and compatibility with existing banking applications.
- All device and behavioural data must be stored and processed exclusively within India. No cross-border data transfer.
- Minimum 6-month behavioural profiles maintained per customer for anomaly detection.

7.11 Reporting and Dashboards

- Pre-packaged MIS dashboards: Fraud trends, investigator performance, channel-wise fraud analytics, false positive rates, detection rates, and SLA compliance.
- Custom report builder with wide range of attributes: transaction, case, customer, account, device, IP.
- Drill-down dashboards with pictorial depiction: graphs, geographical maps, heat maps, trend charts.
- Configurable alert priority classification: Critical, High, Medium, Low.
- Regulatory reports in RBI, NABARD, DFS, and FIU-IND prescribed formats.
- Export to Excel/CSV for offline analysis.
- Concurrent report generation without performance degradation.
- Interactive dashboards tailored to Fraud Analysts, Investigators, Team Leaders, and Senior Management views.
- Daily, Weekly, Monthly, and Quarterly automated reports with configurable distribution.

7.12 Adaptive Authentication and Risk-Based Authentication

- Integration with existing and future authentication processes (SMS/OTP/MFA/Step-Up Authentication/Biometric Authentication) per RBI Authentication Framework Directions 2025.
- Risk-based step-up authentication triggered dynamically based on EFRM risk score.
- Configurable authentication policies based on transaction type, amount, beneficiary risk, device risk, and location risk.
- Zero Trust Architecture principles in authentication decisions.
- Support for TOTP (Time-based One-Time Password), FIDO2, and other modern authentication standards.

7.13 Audit Trail and Log Management

- All system events, user actions, configuration changes, alert/case activities, rule changes, watchlist updates, and API calls must be logged with immutable audit trails.
- Audit logs must include: NTP-synchronized timestamp, User ID, Action Type, Before/After values for configuration changes, Source IP, Session ID, and Outcome.
- Log retention: 5 years online accessible; subsequent years in compressed archival storage retrievable within 24 hours.
- Audit logs must be exportable to each Bank's SIEM/SOC system in real-time or batch mode.
- Read-only auditor access role for external auditors, RBI, NABARD, and regulatory personnel.
- Application-level audit trail for all investigator actions on cases and alerts must be immutable.
- Tamper-proof log integrity verification mechanism.

7.14 Testing Environment and Rule Simulator

- Provide a comprehensive, fully integrated testing environment with rolling historical data for rule simulation. This must be a dynamic environment to replicated real and / or production environment
- Enable parallel testing and performance benchmarking of multiple rules with real-time impact analysis on alerts and false positives.
- Implement comprehensive parameter management, change tracking with maker-checker workflows, version control, and rollback capabilities.
- Support simulations of threshold sensitivity and non-monetary event rules (address change, device changes, PIN resets).
- Provide logical and arithmetic expression builders for scenario creation.
- Support both real-time and batch rule execution with analysis of execution success.

8. Technical Architecture Requirements

8.1 Architecture Principles

- Platform-agnostic solution (not constrained to single hardware/OS/database).
- High Availability at all tiers (Active-Active or Active-Passive). No Single Point of Failure (SPOF) at any application layer.
- Horizontal and vertical scalability without core architecture changes.
- WCAG 2.1 compliance for all user interfaces.
- Support for IPv6 addressing in addition to IPv4.
- Microservices or modular architecture preferred for independent scalability.

8.2 Infrastructure Sizing

- Bank provides IT infrastructure (hardware, OS, database, network). Bidder provides detailed sizing specifications.
- Bidder must provide separate hardware sizing documents for [UPGB] and [GGB].
- Sizing must specify: Hardware, OS, Database, Storage, Network, Middleware requirements; Responsibility Matrix (Bank vs. Bidder); Licensing details.
- CPU, memory, and storage at peak load must not exceed 70% of provisioned capacity.
- If sizing proves inadequate during the contract period, Bidder bears all reconfiguration/upgrade costs.

8.3 DC/DR and Business Continuity

- RTO: ≤ 120 minutes (critical failures). RPO: ≤ 10 minutes (data loss). Zero exceptions.
- Active-Active or Active-Passive DC-DR configuration with automatic failover and zero transaction loss.
- Real-time data replication from DC to DR. Replication lag must be monitored and must not exceed RPO threshold.
- Quarterly DR drills for each Bank independently. DR drill results submitted to respective Bank within 5 business days.
- DR drill demonstrated before Phase 2 Go-Live for each Bank. Go-Live not permitted without successful DR demonstration.
- RTO/RPO test reports mandatory as part of SLA compliance reporting.
- Load balancing across multiple servers/nodes/clusters with transparent failover.
- In case of DC/DR relocation by either Bank, Bidder supports relocation at no additional cost.

8.4 Security Architecture

- AES-256 encryption for all data at rest. TLS 1.3 minimum for all data in transit. Upgradeable to future standards.
- SHA-256/SHA-384/SHA-512 hashing. RSA ≥ 2048 bits for digital signatures.

- All data (transaction, customer, audit logs, device intelligence, behavioural data) stored and processed exclusively within India. Cross-border data transfer strictly prohibited.
- DPDP Act 2023 compliance: data minimisation, purpose limitation, consent management, breach notification obligations.
- Integration with each Bank's SOC: PAM (Privileged Access Management), SIEM (Security Incident and Event Management), DAM (Database Activity Monitoring), Active Directory, AV, and other SOC utilities.
- Role-Based Access Control (RBAC). Separate auditor role with view-only access. Periodic user access review.
- Maker-Checker controls for all critical administrative and scenario configuration changes.
- No default credentials. All system credentials must be changed before production deployment. Password policy aligned with RBI guidelines.

9. Cybersecurity and Compliance

9.1 Mandatory Regulatory Compliance

The solution and the Bidder must comply with all of the following without exception:

Regulation / Standard	Applicable To
RBI Master Directions on Fraud Risk Management (July 15, 2024)	Both Banks
RBI Cyber Security Framework for Banks (2016 and updates)	Both Banks
RBI Authentication Framework Directions, 2025	Both Banks
RBI Master Direction on Digital Payment Security Controls, 2021	Both Banks
RBI Mobile Payment Security Controls	Both Banks
RBI Master Direction on Outsourcing of IT Services (April 2023)	Bidder – as service provider
RBI FREE-AI / AI Governance Guidelines	AI/ML components
RBI Advisory on Software Bill of Materials (SBOM)	Mandatory SBOM submission
NABARD Guidelines for Regional Rural Banks	Both Banks (RRBs under NABARD supervision)
CERT-In Advisories and Information Security Guidelines	Both Banks and Bidder
DFS (Department of Financial Services) Advisories	Both Banks
Digital Personal Data Protection Act, 2023 (DPDP Act)	Both Banks and Bidder
Information Technology Act, 2000 (and amendments)	Both Banks and Bidder
PCI-DSS v4.0 (for card data and card transactions)	Both Banks
ISO 27001:2022 (Information Security Management)	Bidder's organisation
OWASP Secure Development Guidelines	Solution development
GFR 2017 Rule 144(xi) – Border Country Restrictions	Bidder eligibility
CVC Guidelines on Procurement Integrity	Both Banks

9.2 VAPT and Security Testing Requirements

- Bidder must submit a VAPT report from a CERT-In empanelled agency not older than 6 months from bid submission date.
- VAPT scope: SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), Secure Code Review per OWASP guidelines.
- All Critical and High vulnerabilities must be resolved BEFORE Phase 2 Go-Live. Zero exceptions. Go-Live will NOT be permitted if any Critical or High VAPT vulnerability remains open.
- Annual VAPT post Go-Live (minimum). Additional VAPT after each major release.
- Vulnerability remediation timelines: Critical ≤ 7 days; High ≤ 15 days; Medium ≤ 30 days; Low ≤ 60 days.
- VAPT Penalties (per Section III, Para 14): Critical: ₹10,000/week/vulnerability; High: ₹5,000/week/vulnerability; Medium: ₹2,000/week; Low: ₹1,000/week.
- Re-testing by Bidder at no additional cost until closure validated by Bank's appointed auditor.

9.3 Software Bill of Materials (SBOM) – Mandatory per RBI Advisory

- Complete SBOM identifying all direct and transitive software dependencies in the proposed EFRM Solution.
- Disclose all open-source components. Banks' written approval required before deployment of any open-source component.
- Open-source must be from actively maintained projects with commercially viable support and clear licensing.
- Open-source licence compliance mandatory (GPL, MIT, Apache 2.0, etc.). GPL-licensed components that could impose licensing obligations on Bank code are prohibited.
- SBOM to be updated and submitted with each major version release.
- SBOM must include: all components, version details, licence type, known CVEs, and remediation status.

9.4 COMPLIANCE WITH IT & IS SECURITY POLICY:

While Bidder's personnel are performing implementation or maintenance services at Uttar Pradesh Gramin Bank and Gujrat Gramin Bank, the Vendor shall have to comply with the Bank's IT & IS Security policy. Some of the key areas are as under:

1. Responsibilities for data and application privacy and confidentiality
2. Physical and logical separation of customer data from other vendors/applications
3. In general, confidentiality, integrity, and availability must be ensured.
4. The Vendor shall comply with all applicable guidelines issued by RBI, NABARD and other regulatory authorities regarding IS and Cyber Security.
5. The Bank will have the right to conduct audits of the Vendor/service provider, either directly or through its internal/external auditors or authorized third-party agencies during the contract period. The Vendor shall provide full access to relevant systems, records, documents, logs, infrastructure and personnel related to the services rendered to the Bank.
6. The Vendor shall also permit inspection and supervision by RBI, NABARD or any other statutory authority, including access to records and systems, and shall extend full cooperation during such audits or inspections.
7. The Vendor shall ensure that periodic Information Security and Cyber Security audits are conducted (preferably by CERT-In empanelled auditors) and shall ensure timely compliance with the audit observations.
8. Compliance with the provisions of the Digital Personal Data Protection Act, 2023 (DPDP Act) and other relevant act/guideline of Government of State and Government of India.
9. Implementation and compliance of CSITE/CERT-In advisory issued from time to time.

10. The selected bidder shall ensure that the proposed solution undergoes Vulnerability Assessment and Penetration Testing (VAPT) through a CERT-In empanelled auditor. The assessment shall also include Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and secure code review in accordance with OWASP guidelines and secure development practices.
11. All identified vulnerabilities shall be remediated in line with industry best practices, and no Critical or High-risk vulnerabilities shall remain unresolved at the time of phase 2 Go-Live. Detailed assessment reports, along with remediation evidence and closure validation, shall be submitted to the Bank for review and approval.
12. Any deviation from the defined security requirements shall require prior written approval from the Bank, supported by documented risk acceptance, in line with the Bank's internal risk management framework and applicable regulatory guidelines.
13. Post Go-Live, the solution shall undergo periodic VAPT and security assessments as per the Bank's Information Security Policy, regulatory requirements, and audit observations, including but not limited to guidelines issued by the Reserve Bank of India (RBI), CERT-In advisories, and other applicable authorities.
14. Timelines for Remediation:
 - Critical vulnerabilities: within 7 calendar days
 - High vulnerabilities: within 15 calendar days
 - Medium vulnerabilities: within 30 calendar days
 - Low vulnerabilities: within 60 calendar days
15. Penalty for Non-Compliance: In case of failure to remediate vulnerabilities within defined timelines, the Bank shall levy a penalty as mentioned in the section III point no 13.4.
16. Go-Live Dependency: Go-Live shall not be permitted if any Critical or High vulnerabilities remain open. Any exception shall require formal risk acceptance by the Bank's competent authority.
17. Re-testing & Validation: The bidder shall conduct re-testing at no additional cost until closure of identified vulnerabilities is validated by the Bank or its appointed auditor.
18. **The Vendor shall execute and comply with the following agreements / regulatory requirements with the Bank prior to commencement of services:**
 - **Escrow Agreement**
 - **Non-Disclosure Agreement (NDA)**

The details of the Bank's IT & IS Security Policy, covering the key areas, will be shared with the selected Bidder.

10. Implementation Methodology

10.1 Implementation Timeline

Milestone	Activity	Timeline from PO (T)	Deliverable
Project Kick-Off	Project team mobilisation, gap assessment, infrastructure audit at both Banks, SRS finalisation, project plan submission.	T + 14 days	Project Plan, SRS
Phase 1 Installation	Solution installation at both Banks' DC, DR, and UAT environments.	T + 30 days	Installation Report
Phase 2	Integration of channels mentioned under Phase 2	T + 90 days	

Milestone	Activity	Timeline from PO (T)	Deliverable
Phase 2 UAT	Phase 2 channel integrations complete. UAT conducted by each Bank independently. UAT issues resolved.	T + 90 days	UAT Sign-Off (Phase 2)
Phase 2 Go-Live	Phase 2 channels live in production at both Banks' DC and DR. DR drill demonstrated successfully.	T + 90 days	Go-Live Certificate (Phase 2) from OEM
Phase 3	Integration of channels mentioned under Phase 3	T + 120 days	
Phase 3 UAT	Phase 3 channel integrations complete. UAT conducted by each Bank independently. UAT issues resolved.	T + 120 days	UAT Sign-Off (Phase 3)
Phase 3 Go-Live	Full production with all Phase 2 and Phase 3 channels. All channels live at both Banks.	T + 120 days	Go-Live Certificate (Phase 3) from OEM
Final Acceptance	All training complete, escrow established, OEM certification for onsite resources, all documents delivered, VAPT clean report.	T + 150 days	Final Acceptance Certificate
Operations (Ongoing)	24x7x365 FMS support, quarterly DR drills, VAPT, AI/ML model validation, updates, upgrades.	Throughout Contract	Monthly SLA Reports

NOTE: Go-Live timelines for UPGB and GGB run independently. Phase 1 Go-Live of GGB is NOT contingent on Phase 1 Go-Live of UPGB, and vice versa. Delays at one Bank must not affect the other Bank's implementation timeline.

10.2 Cutover and Migration

- Bidder must conduct a comprehensive gap assessment of each Bank's current fraud monitoring infrastructure and submit a Migration/Cutover Plan.
- Cutover Plan must address: data migration (historical alerts/cases if required), rule migration, parallel running period, cutover checklist, rollback plan.
- Parallel running of existing fraud systems (if any) with new EFRMS for minimum 2 weeks before final cutover.
- Zero downtime cutover is required. Cutover to be performed during scheduled maintenance windows.
- Bidder responsible for complete cutover and transition at no additional cost.

11. Onsite Technical Support (FMS) – Requirements

11.1 Support Structure

Level	Qualification	Deployment	Key Responsibilities
L1 Engineer	BE/B.Tech/MCA/BCA/BSc-IT. Min 2 years IT support experience. OEM certified.	24x7x365 at each Bank's premises (UPGB: Lucknow; GGB: Vadodara). Separate dedicated resource per Bank.	User management, daily monitoring, application helpdesk, daily status reports, health monitoring.

Level	Qualification	Deployment	Key Responsibilities
L2 Engineer	BE/B.Tech/MCA/BCA. Min 4 years DB and EFRMS experience. OEM certified.	Business hours/days at DC/DR. On-call 24x7 for P1/P2 incidents.	Rule creation/modification, troubleshooting, RCA, DC-DR sync, data backups, performance tuning, quarterly audit.
L3 Engineer	BE/B.Tech/MCA. Min 6 years IT Security. Min 2 years EFRMS experience. Must be on OEM's payroll.	Onsite for critical issues. Remote otherwise. On-call 24x7.	Critical code changes, VAPT gap closure, version migration, OEM escalation, audit compliance, vulnerability patching, model performance review.

△ IMPORTANT: All L1/L2/L3 resources must be on the direct payroll of OEM/Bidder, not contractual or third-party outsourced. OEM certification mandatory before deployment. 1-month advance notice required for resource replacement with Bank's written concurrence. KYE (Know Your Employee) background verification mandatory for all deployed resources before deployment.

11.2 Scope of L1 Support

L1 would typically address queries and all end user issues pertaining to: Business application related issues/queries, Enterprise applications (In-Scope), Generic IT Queries, Queries related to business process, reports generation, presentation layer applications, etc.

Other environmental software related to the EFRM Solution.

The Bank expects the Bidder to provide for L1 support for all activities and services that are part of scope. The key activities that the bidder is expected to perform as part of Level 1 Helpdesk Support are:

1. User Management.
2. Creation or modification of user profiles.
3. Assessment in case of specific rights assignment.
4. Provision for assigning user rights only for certain fixed period.
5. Periodic user right monitoring (at known frequency) must be specified and implemented.
6. Categorization of requests into functional clarification, bug or change request.
7. Functional clarification / work around to be provided by Level 1 support itself.
8. Bug change requests to be logged and reported for further processing.
9. Resources should perform daily monitoring and submit status reports and other reports as per bank's requirements.
10. Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates.
11. Monitoring overall health of the solution and analyse all events and logs.

11.3 Scope of L2 Support

The Bank expects the Bidder to provide L2 support for all activities and services that are part of the scope.

The L2 support provided by the Bidder should be comprehensive and cover entire management and support of the EFRM solution provided by the Bidder. The resource should also coordinate for all third- party solutions provided by the Bank to ensure smooth functioning of the EFRM solution.

The services specified herein are not exhaustive and only indicative:

1. Provide continuous onsite support for the EFRM solution provided by the bidder.
2. Creation/ Modification of rules/policies through the proposed solution based on the requirement of Bank.

Joint RFP for EFRM solution for UPGB and GGB

3. Knowledge of how to configure the customize dashboard and reports.
4. Troubleshoot real time, NRT, batch processing activities at various levels in the EFRM Solution.
5. Troubleshoot any query processing activity at various levels in the EFRM Solution.
6. Resolve the call within stipulated timeframe as defined in Service Level Agreement.
7. Coordinate with the L3 teams for resolution and provide necessary information as may be required by the team to resolve the issues.
8. Escalate the unresolved calls as per escalation matrix.
9. Automatically log in calls during escalation.
10. Provide the timeframe for providing a solution of resolution of the escalated calls.
11. Prepare a root cause analysis document with the resolutions provided for major issues such as:
 - Production issues
 - Problems which have resulted in complete service disruptions or downtime
 - Delayed response times
 - Data / table corruptions
 - System Performance issues (high utilization levels)
12. The Onsite resources will be responsible for ensuring the DC-DR sync, regular maintenance of application Logs and also Continuous monitoring of solution.
13. The onsite resources should have the capability to support archiving the data on HDD/ Peripherals, performing integrity checks and retrieve from the above for the purpose of processing.
14. The onsite resources will be responsible for performing data backups, performing integrity checks and ensuring the integrity of the backup. The bank will provide the required backup solution and tapes to facilitate this process.
15. Liaise with the L1 support personnel for the call information and resolution.
16. All other activities as would be required by the Bidder to manage and maintain the solutions.
17. Perform the application audit on a quarterly basis or as per the guidelines of the bank.
18. Rectify any corruption in the software.
19. Ensure patch releases are ported to the production environment with no business disruption or business losses.
20. Support quarterly BCP/DR drills.
21. The resources shall be responsible to create/configure and customize the solution as per Bank's requirement.
22. Provide application support from the Bank's data centre as mentioned above for the Data centre and disaster recovery site.
23. Routing the transactions through the backup system in case the primary system fails.
24. Support for integrating any applications that need to be interfaced with the EFRM solution in the future.
25. Level 2 service desk agents would need to be deployed by the bidder at DC/DR/Office premises from where the Level 2 support is planned to be provided. The bidder is expected to act upon the tickets routed from Level 1. The bidder has to ensure that proficient and professional personnel are put to handle the L2 support and resolutions are provided on a proactive basis.

The L2 helpdesk resources proposed should have adequate and relevant experience in the areas mentioned like database and EFRMS application. The Bank has a right to review and reject

resources whose competency levels are below expectations. Support and maintain all interfaces to the EFRMS and other solutions part of this scope document modifications to existing scripts, reports presentation to Bank management on the critical issues reported, resolved, solution provided and the suggested recommendations or leading practices as and when asked by the Bank or on a monthly basis whichever is earlier. Perform performance tuning of the applications mentioned in the Scope of Work of this document including Solution tuning.

11.4 Scope of L3 Support

Critical code level changes or application software related issues. This support is required for all components that are expected to be provided by the Bidder as part of this RFP.

The Bidder has to provide the resolution / service as per the defined service levels in this RFP. The Bidder has to make sure that the methodology proposed for addressing and resolving problems is aligned to the required and defined service levels.

The Bidder should staff the service desk with persons who are conversant with the solutions deployed and are capable of resolving routine problems and queries through the service desk application or over the phone. The staffing needs of the service desk will be decided by bank based on calls/ticket volumes and patterns.

Brief description of the envisaged activities to be performed by Bidder at L3 is enumerated as under. The services specified herein are not exhaustive and are only indicative:

1. Creation/Modification of rules/policies through the proposed solution based on the requirement of the Bank.
2. Resolve the call within the stipulated timeframe as defined under the service level agreements.
3. Communicate the status of the call to the Bank and accordingly update the status, resolution or workaround and date of resolution.
4. Prepare a root cause analysis document for issues referred to L3 support and provide to the Bank along with the resolution.
5. Liaise with the L2 support personnel for the call information and resolution.
6. Provide version upgrades for EFRMS application.
7. The resources shall be responsible to close the audit gaps, if found in the third party audit report shared by the Bank during the entire contract period.
8. The L3 resource shall be responsible for proactively closing the vulnerabilities and Internal Information System's Audit observations related to the EFRMS system to make the system resilient to cyber threats in the mentioned TAT defined by the Bank.
9. L3 support shall be responsible for Patching of the proposed EFRM solution with the latest available patches.
10. All other activities as would be required by the SI to manage and maintain the solutions.
11. Perform Version Migration - The services specified herein are not exhaustive and only indicative.
12. Perform version migration as per the version release plan of OEM and agreed by the Bank.
13. Version upgrades and migrations should also include porting of existing customizations.
14. L3 will be responsible for Lodging any unresolved issues with the OEM and providing the solution within the defined time frame.
15. Onsite L3 resource will be responsible for supervising: the DC-DR sync, regular maintenance of application Logs and also Continuous monitoring of solution.
16. Onsite L3 resource should supervise: the archiving process of data on HDD/ Peripherals, integrity checks and retrieval.
17. Onsite L3 resource will be responsible for supervising: data backups, integrity of the backup. The bank will provide the required backup solution and tapes to facilitate this process.

11.5 Training Requirements

- Pre-UAT Training (mandatory): Minimum 5 working days at each Bank's location before Phase 2 UAT. Conducted by OEM resources only. Covers: Technical (IT team), Functional (Fraud Analysts), and Administrative (System Admins) training.
- Annual Training: Minimum 5 working days per year per Bank during the contract period. Separate technical and functional tracks.
- Training materials in English, customised with Bank-specific architecture and configurations.
- Training locations: UPGB HO Lucknow; GGB HO Vadodara. Joint sessions permissible with mutual consent.
- Updated SOPs, User Manuals, and Training Materials provided at each version upgrade at no additional cost.
- No additional cost will be paid for pre-UAT and annual training.

12. Upgrades and Updates

- All major and minor version upgrades must be provided at no additional cost during the contract period.
- Minor version: small incremental version/patching per OEM/OSD product release plan. Covered under ATS.
- Major version: significant new features or architecture changes. Bidder must migrate including porting of all existing customisations at no additional cost.
- RBI/NABARD-mandated rule updates and compliance changes must be implemented at no additional cost within the timelines specified by the respective regulator.
- 500 annual rule customisations included under ATS at no additional cost per Bank.
- Any additional customisations beyond 500/year charged at the per-person-day rate specified in the Commercial Bid.
- All upgrades must be tested in UAT environment and Bank sign-off obtained before production deployment.

13. Service Level Agreement (SLA) and Penalties

13.1 System Availability SLA

After Go-Live of the solution, penalty will be deducted for partial or complete downtime of the solution provided as below.

Vendor will have to guarantee a minimum uptime of 99.90%, calculated on a quarterly basis. Application availability will be 99.90% on 24x7x365. The penalty will be calculated as per the details given below.

Uptime percentage - 100% less Downtime Percentage

Downtime percentage - Unavailable Time divided by Total Available Time, calculated on a quarterly basis.

Total Available Time — 24hrs per day for seven days a week excluding planned downtime
Unavailable Time - Time involved while the solution is inoperative or operates inconsistently or erratically.

Availability (Quarterly)	Penalty per Bank per Year
Availability ≥ 99.90%	No Penalty
99.50% ≤ Availability < 99.90%	1% of annual license fee for that Bank for the year

Availability (Quarterly)	Penalty per Bank per Year
98.50% ≤ Availability < 99.50%	2% of annual license fee for that Bank for the year
Availability < 98.50%	2% base + additional 1% per 0.1% below 98.50%
Availability < 98.00% for > 2 consecutive months	Bank may: (a) invoke PBG; (b) terminate contract with 30 days' notice; and/or (c) blacklist Bidder

13.2 Response Time SLA

Condition	Penalty per Bank
≤100 ms for all transactions	No Penalty
>100 ms: 50,000 to 100,000 transactions/day in breach	0.05% of annual license fee per Bank per year
>100 ms: >100,000 transactions/day in breach	0.10% of annual license fee per Bank per year

Hardware sizing has to be provided by bidder based on the TPS proposed by bank and Hardware will be provided accordingly and solution should respond back to source channel within maximum of 100 milliseconds, no penalty will be levied if the solution is unable to respond due to hardware failure or network time out from source channels.

The uptime percentage would be calculated on quarterly basis and the calculated penalty amount would be adjusted from every subsequent Half yearly license payment.

Penalty due to downtime, during contract period will be deducted from any subsequent payment to be made to the Successful bidder.

13.3 Incident Resolution SLA

Priority	Description	Resolution TAT	Penalty per Incident
P1 – Critical	EFRMS completely down. All channels unavailable. Data loss risk.	2 hours	₹50,000 per hour delay beyond TAT per Bank
P2 – High	Major channel unavailable (e.g., UPI or Debit Card monitoring down). Major feature loss.	4 hours	₹25,000 per hour delay beyond TAT per Bank
P3 – Medium	Significant performance degradation. Non-critical feature unavailable.	8 hours	₹10,000 per hour delay beyond TAT per Bank
P4 – Low	Minor cosmetic or non-impacting issues.	24 hours	₹5,000 per day delay beyond TAT per Bank

13.4 Vulnerability Remediation and Audit Gap Penalties

Issue Type	Severity	Resolution TAT	Penalty
VAPT Vulnerability	Critical	7 calendar days	₹10,000 per week per vulnerability post deadline

Issue Type	Severity	Resolution TAT	Penalty
VAPT Vulnerability	High	15 calendar days	₹5,000 per week per vulnerability post deadline
VAPT Vulnerability	Medium	30 calendar days	₹2,000 per week post deadline
VAPT Vulnerability	Low	60 calendar days	₹1,000 per week post deadline
IS Audit Gap	Critical	7 working days	₹10,000 per day post deadline
IS Audit Gap	High	10 working days	₹5,000 per day post deadline
IS Audit Gap	Medium	20 working days	₹2,000 per day post deadline
IS Audit Gap	Low	30 working days	₹1,000 per day post deadline
L1 Resource Absence	N/A	Must be present all shifts	₹5,000 per absent engineer per day
Missed DR Drill	N/SA	Quarterly mandatory	₹50,000 per missed drill per Bank
Implementation Delay	N/A	Per agreed phase schedule	1% of phase implementation cost per week. Maximum 10% of TCO.
Escrow Default	N/A	Quarterly update mandatory	₹1,00,000 per quarter of default

△IMPORTANT: All penalties are concurrent and independent. Total aggregate penalty under all heads per Bank shall not exceed 10% of that Bank's total TCO. Upon reaching 10% TCO, the respective Bank may terminate contract and invoke PBG. Phase 2 Go-Live shall NOT be permitted if any Critical or High VAPT vulnerabilities remain open.

Penalty for delay in issue Resolution

Resolution of the problem is expected within 24 hours of escalation by the Bank as per the support matrix provided by the Bidder. Delay in providing resolution will attract penalty at 1% of the license fee pertaining to corresponding year cost per week of delay or part thereof subject to a maximum of 10% of the TCO.

Penalty Due to non-availability of resources during Maintenance Period

In case, if any of the required onsite technical support engineer(s) (L1) is/are not available in any of the shifts on any particular day then a penalty of Rs 5000/- per day will be charged to Bidder and same will be deducted from OTS charges payable to Bidder.

Penalty Due to non-availability of resources during Implementation Period

In the absence of the OEM engineer, suitable replacement from the OEM is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.5% of the Implementation cost, for each day, up to a maximum of 10% of TCO.

Penalty due to erroneous behavior of the Solution

If the solution or any of its components behaves erroneously which results in monetary or business loss to the Bank, then the entire amount of such loss shall be recovered from the bidder on actual basis.

Note:

If **uptime** less than 98.00% due to performance issues continues for more than two months due to any reason at application/solution side, Bank may choose any or all the options like Review the contract, Cancel the Purchase Order, Terminate the Contract, Forfeit the Performance Bank Guarantee and Blacklist the bidder.

SLA will be monitored on Monthly basis. Penalty due to downtime/service unavailability/disruption and any clauses mentioned above during contract period will be deducted from any subsequent payment to be made to the bidder.

Penalty as mentioned above can be levied simultaneously. Maximum deducted penalty of one type will not affect any other type of penalty i.e. all types of penalties can be levied up to their maximum limit simultaneously. However, the total penalty amount, under all heads, cannot exceed 10% of TCO as per RFP.

Bank reserves the right to Cancel the Purchase Order, Terminate the Contract, Forfeit the Performance Bank Guarantee and Blacklist the bidder, in case the bidder exceeds the threshold limit of Delay for any of the items above and/or penalty amount exceed as mentioned above. Bank, at its sole discretion, may exercise any or all the options against the bidder, in such circumstances.

However, any penalty imposed by the Govt. or any other statutory body due to act/failure of conduct/leakage of data by selected bidder or its agents shall be entirely borne by the bidder. Once the maximum limit of the penalty is reached, the Bank may consider termination of the contract, after invoking Performance Bank Guarantee submitted by the bidder.

Bank may recover such amount of penalty from any payment being released to the successful bidder, irrespective of the fact whether such payment is related to this contract or otherwise.

All Services Level Agreement (SLAs) shall undergo a comprehensive review every six months. This review will be based on prevailing industry best practices and conducted in consultation with the successful bidder. Notwithstanding, the bank retains the ultimate authority to make final determinations regarding any modifications or updates to the SLAs. The decisions made by the bank in this regard shall be conclusive and binding.

14. Contract Terms

14.1 Contract Period

The contractual period will be: Implementation Period (maximum 120 days from PO date) + 5 Years from Phase 2 Go-Live for each Bank independently. Any delay during the implementation period will not shorten the 5-year operational period. Contract periods for UPGB and GGB run independently and are separately measured.

At the end of the 5-year period, each Bank, at its sole discretion, may extend the contract for an additional 2 years on mutually agreed terms and pricing.

During the contract period organic as well as inorganic growth, the volume and number of transactions will not make any impact of price of solution / commercial.

14.2 Payment Terms

Milestone	% of Table-B Implementation, Integration, and Configuration Cost	Notes
Contract signing + solution delivered to DC & DR (Phase 1)	10%	Within 15 days of completion of Phase 1. No advance.
Phase 2 UAT Sign-off	25%	After Bank's written UAT sign-off.
Phase 2 Production Go-Live Sign-off	25%	After Bank's written Go-Live sign-off.
Phase 3 UAT Sign-off	20%	After Bank's written UAT sign-off.
Phase 3 Production Go-Live Sign-off	15%	After Bank's written Go-Live sign-off.
Final Acceptance (all training, escrow, OEM cert, docs)	5%	After Final Acceptance Certificate.

- Table-A (License + AMC) and Table-C (OTS/FMS): Paid quarterly in advance from Phase 2 Go-Live. Annual fees in Year 2 onwards payable half-yearly in advance.
- All invoices in INR. Digitally signed invoices to be submitted to Bank within 30 days of month-end/quarter-end.
- Payment within 30 working days of undisputed invoice receipt. Disputed invoices resolved within reasonable time; payment within 30 working days of dispute resolution.
- Bank may withhold payment commensurate with SLA penalties due. Bank's sign-off required before each payment milestone is triggered.
- TDS deducted at applicable rates. GST paid at applicable rates on submission of valid GST invoice.
- No advance payment. Bank will not pay any amount before the corresponding milestone is achieved and accepted in writing.

14.3 Escrow Arrangement

Both Banks, individually or jointly, and the successful bidder with OEM shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code for the EFRM solution supplied by the successful bidder to the Bank to protect its interests in an eventual situation. The Bank and the successful bidder and OEM shall enter into escrow agreement with the designated escrow agent, which will set out, inter- alia, the events of the release of the source code and the obligations of the escrow agent. As a part of the escrow arrangement, the successful bidder and OEM is expected to provide a detailed code documentation of the customization. The Escrow arrangement suggested by the successful bidder shall not be binding on the Bank. The Bank reserves the right to explore alternate escrow mechanisms based on the Bank's existing practices. The Bank and the successful bidder may enter such escrow arrangement that is mutually agreed upon by the two parties. The source code of customizations done by the successful bidder on the latest version of the application software under the proposed solution running in the bank is to be kept in escrow at least once in a quarter. The escrow will be released to and become the property of the Bank if the agreement is terminated for either default or insolvency or should the bidder/ OEM cease or give notice of intention to cease to provide maintenance or technical support service for the software as required by the agreement. All payment and costs with respect to lodging of software with escrow services in India would be borne by the successful bidder. The cost of escrow and other related costs will be borne by bidder.

14.4 Sub-Contracting

Sub-contracting of core EFRM implementation, integration, and ongoing support is PROHIBITED. Sub-contracting of non-core activities (e.g., hardware logistics, facility management) requires prior written approval of BOTH Banks. In all cases, the Bidder remains fully accountable for all services. KYE and background verification mandatory for all sub-contractor resources. Any violation of sub-contracting restrictions shall constitute a material breach.

15. Deliverables

S.No.	Deliverable	Due Timeline
1	Detailed Solution Architecture Document and Hardware Sizing for both Banks (DC + DR separately)	Within 14 days of PO
2	Software Bill of Materials (SBOM) – all direct and transitive dependencies	With Technical Bid; updated at each major release
3	Source Code Audit Evidence (vulnerability-free, secure coding from CERT-In empanelled agency)	Within 30 days of PO
4	VAPT Assessment Report (CERT-In empanelled, ≤6 months old from bid date)	With Technical Bid; before each Go-Live
5	High Level Design (HLD) + Low Level Design (LLD) Documents	Before Phase 2 UAT
6	System Requirements Specification (SRS) Document	Before Phase 2 UAT
7	Integration Design Documents (per channel, per Bank)	Before respective channel integration
8	Test Plans, Test Cases (Unit, Integration, SIT, UAT, Performance, Load) per Bank	Before each UAT phase
9	Deployment Plan per Bank	Before each Go-Live phase
10	User Management Guide, Administration Guide, Content Management Guide	Before Phase 2 Go-Live
11	Security Guide and Data Flow Architecture Document	Before Phase 2 Go-Live
12	Training Manuals (Technical and Functional) – Bank-specific	Before Pre-UAT Training
13	Go-Live Certificate (Phase 2) – signed by OEM	After Phase 2 Go-Live
14	Go-Live Certificate (Phase 3) – signed by OEM	After Phase 3 Go-Live
15	AI/ML Model Documentation and Model Risk Register	Before Phase 2 Go-Live; updated semi-annually
16	DR Drill Results Report per Bank	After each quarterly drill
17	Vendor BCP Plan for resource and service continuity	Before Phase 3 Go-Live
18	Data Archival and Retrieval Strategy Document	Before Phase 3 Go-Live
19	OEM Certification for All L1/L2/L3 Onsite Resources	Before resource deployment
20	Final Acceptance Certificate (all phases complete)	After Phase 3/Final Acceptance
21	Quarterly SLA Performance Reports (per Bank)	Quarterly throughout contract
22	Annual Performance Review Report (SLA, False Positive Rate, Detection Rate)	Annually

16. Legal and Governance Provisions

16.1 Governing Law and Jurisdiction

[Contract / Master Agreement] This Master Service Agreement shall be governed by the laws of India. Disputes arising under the Joint Master Agreement: Courts in Lucknow.

[UPGB Statement of Work] UPGB-specific disputes and enforcement: Courts in Lucknow, Uttar Pradesh.

[GGB Statement of Work] GGB-specific disputes and enforcement: Courts in Vadodara, Gujarat.

16.2 Arbitration

If any dispute or difference of any kind whatsoever shall arise between the Bank and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

If the parties fail to resolve their disputes or difference by such mutual consultation within a period of 30 days, then either the Bank or the supplier may give notice to the other party of its intention to commence arbitration, as hereinafter provided, as to the matter in dispute, and no arbitration in respect of this matter may be commenced unless such notice is given.

Any dispute or difference in respect of which a notice of intention to commence arbitration has been given in accordance with this clause shall be finally settled by arbitration. Arbitration may be commenced prior to or after delivery of the goods under the contract. Arbitration proceedings shall be conducted in accordance with the following rules of procedure.

The dispute resolution mechanism to be applied shall be as follows:

In case of dispute or difference arising between the Purchaser and a Supplier relating to any matter arising out of or connected with the agreement, such dispute or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The arbitral tribunal shall consist of 3 arbitrators one each to be appointed by the Purchaser and the Supplier; the third Arbitrator shall be chosen by the two Arbitrators so appointed by the Parties and shall act as Presiding Arbitrator. In case of failure of the two arbitrators appointed by the parties to reach upon a consensus within a period of 30 days from the appointment of the presiding Arbitrator, the Presiding Arbitrator shall be appointed by the Uttar Pradesh Gramin Banks and Gujrat Gramin Bank, India which shall be final and binding on the parties.

If one of the parties fails to appoint its arbitrator within 30 days after receipt of the notice of the appointment of its Arbitrator by the other party, then the Uttar Pradesh Gramin Banks and Gujrat Gramin Bank shall appoint the Arbitrator. A certified copy of the order of the Uttar Pradesh Gramin Banks making such an appointment shall be furnished to each of the parties.

Arbitration proceedings shall be held at Lucknow or Vadodara, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English. The decision of the majority of arbitrators shall be final and binding upon both parties. The cost and expenses of Arbitration proceedings will be paid as determined by the Arbitral Tribunal. However, the expenses incurred by each party in connection with the preparation, presentation etc. of its proceedings as also the fees and expenses paid to the arbitrator appointed by such party or on its behalf shall be borne by each party itself.

Where the value of the contract is Rs. 10 million and below, the disputes or differences arising shall be referred to the Sole Arbitrator. The Sole Arbitrator shall be appointed by agreement between the parties; failing such agreement, by the appointing authority namely the Uttar Pradesh Gramin Banks'.

Notwithstanding any reference to arbitration herein,

Joint RFP for EFRM solution for UPGB and GGB

- I. The parties shall continue to perform their respective obligation under the contract unless they otherwise agree; and
- II. The Bank shall pay the supplier any monies due to the supplier.
- III. Submitting to arbitration may be considered as an additional remedy and it does not preclude Parties to seek redressal/ other legal recourse.
- IV. Coverage of Successful Bidder under the Employees' Provident Funds and Miscellaneous Provisions Act, 1952 (this clause will be relevant only when the successful bidder is required to provide human resources to the Bank under the contract)
- V. The Successful bidder has to submit necessary details of all the outsourced employees for any type of services engaged either through contractors or directly whenever required by the Bank. If engaged through contractors, list of all the contractors engaged for any/all services and whether the said contractors are covered independently under the EPF & MP Act 1952 is to be submitted on the Bank's request. The agreement of contracts with the contractors, the PF code number of the contractors, if covered, the attendance of the contract employees, the remitted PF challan with the Electronic Challan cum Return (ECR) should be submitted on the Bank's request.

16.3 Confidentiality and Non-Disclosure Agreement

The Bidder and its employees, subcontractors, agents, and representatives shall treat all Bank data, information, business processes, and system configurations as strictly confidential. The Bidder shall execute a Non-Disclosure Agreement (NDA) with each Bank as per **Annexure-VI** within 30 days of PO issuance. The NDA obligations shall survive contract termination without time limit, except for information that enters the public domain through no fault of the Bidder. The Bidder shall ensure that all personnel deployed under this contract sign individual NDAs before commencement of work.

16.4 Intellectual Property Rights

All application and software must be properly licensed during the period of the contract. Bank may demand evidence of the same. While the successful bidder/ OEM shall retain the intellectual property rights for the application software, it is required that successful bidder shall grant user-based/transaction-based/account-based subscription License for the term to the bank for the bank's exclusive use without limitation on the use of those licenses to any number of source channels.

The successful bidder shall place the source code of customizations done for the bank in Banks environment (and the procedures necessary to build the source code into executable form) for the application software, and the source code of the application software in escrow with a reputable agency (a bank or established software escrow firm in India) acceptable to the Bank during the contract period.

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

Bidder warrants that the inputs provided and/or deliverables supplied by them does not and shall not infringe upon any third-party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever.

In the event that the Deliverables become the subject of claim of violation or infringement of a third

party's intellectual property rights, bidder shall at its choice and expense: [a] procure for the project the right to continue to use such deliverables; [b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; However, Bank shall not bear any kind of expense, charge, fees or any kind of costs in this regard. Notwithstanding the remedies contained herein, the bidder shall be responsible for payment of agree in case service levels are not met because of inability of the bank to use the proposed product.

The indemnification obligation stated in this clause apply only in the event that the indemnified party provides the indemnifying party prompt written notice of such claims, grants the indemnifying party sole authority to defend, manage, negotiate or settle such claims and makes available all reasonable assistance in defending the claims at the expenses of the indemnifying party. Notwithstanding the foregoing, neither party is authorized to agree to any settlement or compromise or the like which would require that the indemnified party make any payment or bear any other substantive obligation without the prior written consent of the indemnified party. The indemnification obligation stated in this clause reflects the entire liability of the parties for the matters addressed thereby.

The bidder acknowledges that business logics, workflows, delegation and decision-making processes of Bank are of business sensitive nature and shall not be disclosed/referred to other clients, agents or distributors.

16.5 Data Ownership, Privacy and Security

All transaction data, customer data, case data, operational data, audit logs, device intelligence data, and behavioural data is the exclusive property of the respective Bank. The Bidder shall not access, use, share, transfer, or retain such data for any purpose other than performance of contracted services. Data breach is a material contract violation entitling the affected Bank to terminate and invoke PBG.

The Bidder must comply with all obligations under India's Digital Personal Data Protection Act, 2023 (DPDP Act) including: data principal rights (access, correction, nomination, deletion within regulatory retention requirements); consent management framework; data breach notification to both the Bank and the Data Protection Board within prescribed timelines.

All data must be stored and processed exclusively within India. Cross-border data transfer is strictly and absolutely prohibited.

16.6 Amalgamation / Restructuring Clause

If either Bank undergoes a merger, amalgamation, takeover, consolidation, reconstruction, or any change of ownership, this Agreement shall be deemed automatically assigned to the successor entity. All Bidder obligations, SLAs, pricing, and contractual conditions shall continue unchanged for the remaining contract period. The Banks' decision regarding the successor entity shall be final and binding on the Bidder. This provision is particularly relevant given the recent amalgamation histories of both UPGB and GGB.

16.7 Limitation of Liability

Bidder's aggregate liability under the contract shall be limited to the total contract value (TCO) of the respective Bank. The following are specifically EXCLUDED from this limitation and shall have uncapped liability:

- Liability for Personally Identifiable Information (PII) data breaches caused by Bidder's negligence or wilful misconduct.
- Third-party claims for Intellectual Property Rights infringement.

- Wilful misconduct or gross negligence by the Bidder, its employees, or agents.
- Regulatory penalties imposed on either Bank directly attributable to Bidder's failure to comply with regulatory requirements.
- Fraud or criminal acts by Bidder's personnel.

16.8 Indemnity

The Bidder (the "Indemnifying Party") shall indemnify, defend, and hold harmless each Bank (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes, and damages arising from: (a) bodily injury, death, or damage to property attributable to the Bidder's negligence or wilful default; (b) third-party claims that any service or product provided infringes a copyright, trade secret, or patent; (c) data breaches caused by Bidder's negligence or wilful misconduct; (d) failure to comply with applicable regulatory requirements.

16.9 Force Majeure

The Successful Bidder shall not be liable for forfeiture of its Performance Security, imposition of liquidated damages, or termination for default if and to the extent that its delay in performance or other failure to perform its obligations under the Contract is the result of an event of Force Majeure.

For the purposes of this clause, 'Force Majeure' means any event beyond the reasonable control of the Successful Bidder and not involving its fault or negligence and which was not reasonably foreseeable. Such events may include, but are not limited to, acts of Government or regulatory authorities, war, revolution, fire, flood, epidemic, quarantine restrictions, freight embargoes, or natural calamities. Delay or failure by subcontractors or suppliers of the Successful Bidder shall not constitute a Force Majeure event.

If a Force Majeure situation arises, the Successful Bidder shall promptly notify the Bank in writing of such condition and the cause thereof, but in any case not later than ten (10) days from the commencement of such event. The Successful Bidder shall provide reasonable evidence of the occurrence and impact of the Force Majeure event. Unless otherwise directed by the Bank in writing, the Successful Bidder shall continue to perform its obligations under the Contract as far as reasonably practicable and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

If the impossibility of performance continues for a period exceeding six (6) months, either party may terminate the Contract wholly or partially by giving thirty (30) days' prior written notice to the other party. Upon such termination, neither party shall have any further liability except for payment for goods or services already delivered and accepted, or for reasonable transition/handover obligations to an incoming vendor or service provider.

16.10 Termination

Termination for Convenience:

Either Bank, by 90 days' written notice sent to the Successful bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the bank's convenience, the extent to which the performance of the Successful bidder under the Contract is terminated, and the date upon which such termination becomes effective.

Termination for Default:

Either Bank may terminate with a 90-day cure notice if the Bidder fails to deliver contracted services, materially breaches contractual obligations, or engages in corrupt or fraudulent practices.

If the Bidder fails to cure within 90 days, the respective Bank may terminate, procure replacement services at the Bidder's cost, and invoke PBG.

Termination for Insolvency:

The Bank, without prejudice to any other remedy for breach of contract, by 90 days' written notice of default sent to the Supplier, may terminate this Contract in whole or in part:

- a. if the successful bidder fails to deliver any or all the Goods and Services within the period(s) specified in the Contract, or within any extension thereof granted by the Purchaser.
- b. if the successful bidder fails to perform any other obligation(s) under the Contract.
- c. If the successful bidder, in the judgement of the Purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.
- d. In case of successful Bidders revoking or cancelling their Bid or varying any of the terms in regard thereof without the consent of the Bank in writing.

'For the purpose of this clause:

- **"Corrupt practice"** means the offering, giving, receiving or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution; and
- **"Fraudulent practice"** means a misrepresentation of facts to influence a procurement process or the execution of a contract to the detriment of the Bank and includes collusive practice among Bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the Bank of the benefits of free and open competition.

In the event the Bank terminates the Contract in whole or in part, the Bank may procure the Goods or Services similar to those undelivered, upon such terms and in such manner as it deems appropriate, and the Supplier shall be liable to the Bank for any excess costs paid/ to be paid by the Bank for such similar Goods or Services. However, the Supplier shall continue performance of the Contract to the extent not terminated.

Exit Obligations:

Upon notice of termination, the Bidder must: (a) support transition for up to 6 months at contracted pricing; (b) provide complete source code, configurations, documentation, and data to the respective Bank within 30 days of termination; (c) certify in writing that all Bank data has been irreversibly deleted from all Bidder systems within 30 days.

16.11 Representation and Warranties

The Bidder represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

That the representations made by the Bidder in its Bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the duties, obligations and responsibilities as laid down in the RFP and unless the Bank specifies to the contrary, the Bidder shall be bound by all the terms of the RFP.

That all the representations and warranties as have been made by the Bidder with respect to its Bid and Contract, are true and correct, and shall continue to remain true and correct through the term of this Contract.

That the execution of the Services herein is and shall be in accordance and in compliance with all applicable laws.

That there are –

1. no legal proceedings pending or threatened against Bidder or any sub Bidder/third party or its team which adversely affect/may affect performance under this Contract; and
2. no inquiries or investigations have been threatened, commenced or pending against Bidder or any sub-Bidder / third part or its team members by any statutory or regulatory or investigative agencies.
3. That the Bidder is validly constituted and has the corporate power to execute, deliver and perform the terms and provisions of this Contract and has taken all necessary corporate action to authorize the execution, delivery and performance by it of the Contract.
4. That all conditions precedent under the Contract has been complied by the bidder.

5. That neither the execution and delivery by the Bidder of the Contract nor the Bidder's compliance with or performance of the terms and provisions of the Contract:
 - Will contravene, any provision of any applicable law or any order, writ, injunction or decree of any court or government authority binding on the Bidder,
 - Will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Bidder is a Party or by which it or any of its property or assets is bound or to which it may be subject, or
 - Will violate any provision of the Memorandum or Articles of Association of the Bidder.
6. That the Bidder certifies that all registrations, recordings, filings and notarizations of the bid documents/ agreements/ contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the Bidder which is necessary to ensure the legality, validity, enforceability or admissibility in evidence of the Contract have been/ shall be made.

That the Bidder confirms that there has not and shall not occur any execution, amendment or modification of any agreement/contract without the prior written consent of the Bank, which may directly or indirectly have a bearing on the Contract or the project.

7. That the Bidder owns or has good, legal or beneficial title, or other interest in the property, assets and revenues of the Bidder on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.
8. That the Bidder owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all Intellectual Property Rights, which are required or desirable for the project and the Bidder does not, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. None of the Intellectual Property or Intellectual Property Rights owned or enjoyed by the Bidder or which the Bidder is licensed to use, which are material in the context of the Bidder's business and operations are being infringed nor, so far as the Bidder is aware, is there any infringement or threatened infringement of those Intellectual Property or Intellectual Property Rights licensed or provided to the Bidder by any person. All Intellectual Property Rights (owned by the Bidder or which the Bidder is licensed to use) are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required by the bidder to maintain the same in full force and effect have been taken thereon and shall keep the Bank indemnified in relation thereto.
9. Any intellectual property arising during the course of the execution under the contract related to tools/ systems/ product/ process, developed with the consultation of the bidder will be intellectual property of the Bank.

16.12 Conflict of Interest

The Bidder must disclose any actual or potential conflict of interest at any stage of the procurement or contract performance. If the Bidder fails to disclose and a conflict is subsequently discovered, both Banks may disqualify the Bidder during procurement or terminate the contract during execution.

16.13 Pre-Contract Integrity Pact

Bidders shall submit Pre-Contract Integrity Pact (IP) along with the technical bid as per [Annexure-V](#) of the RFP. Pre-Contract Integrity Pact is an agreement between the prospective bidders and the Bank committing the persons/officials of both the parties not to exercise any corrupt influence on any aspect of the contract. Any violation of the terms of Pre-Contract Integrity Pact would entail disqualification of the bidders and exclusion from future business dealings.

The Pre-Contract Integrity Pact begins when both parties have legally signed it. Pre-Contract Integrity Pact with the successful bidder(s) will be valid till 12 months after the last payment made under the contract. Pre-Contract Integrity Pact with the unsuccessful bidders will be valid till 6

months after the contract is awarded to the successful bidder.

Adoption of Pre-Contract Integrity Pact

The Pact essentially envisages an agreement between the prospective bidders and the Bank, committing the persons /officials of both sides, not to resort to any corrupt practices in any aspect/ stage of the contract.

Only those bidders, who commit themselves to the above pact with the Bank, shall be considered eligible for participate in the Bid. The Bidders shall submit signed Pre-Contract integrity pact as per the [Annexure-V](#). Those Bids which are not containing the above are liable for rejection.

Foreign Bidders to disclose the name and address of agents and representatives in India and Indian Bidders to disclose their foreign principles or associates.

Bidders to disclose the payments to be made by them to agents/brokers or any other intermediary. Bidders to disclose any transgressions with any other company that may impinge on the anti-corruption principle.

Pre-Contract Integrity Pact in respect this contract would be operative from the stage of invitation of the Bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

The Pre-Contract Integrity Pact Agreement submitted by the bidder during the Bid submission will automatically form the part of the Contract Agreement till the conclusion of the contract i.e. the final payment or the duration of the Warranty /Guarantee/AMC if contracted whichever is later.

Integrity Pact, in respect of a particular contract would be operative from the stage of invitation of bids till the final completion of the contract. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

Pre-Contract Integrity Pact shall be signed by the person who is authorized to sign the Bid.

The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

Shri Bishwamitra Pandey
Flat No. 1104, Tower No. KNG-001
JP Greens Wish Town Klassic Sector-134
Email Id- vishwamitram1@gmail.com

Shri Anup Kumar Nayak, IFoS (Retd.)
e-mail- anupnaya@gmail.com Email Id-
vishwamitram1@gmail.com

Any Change in law / policy / circular relating to Pre-Contract Integrity Pact which vitiate the agreement shall accordingly be applicable with immediate effect on written intimation from the Bank.

Any violation of Pre-Contract Integrity Pact would entail disqualification of the bidders and exclusion

from future business dealings, as per the existing provisions of GFR, 2017, Prevention of Corruption Act (PC Act), 1988 or other Financial Rules as may be applicable to the Bank.

16.14 Insurance

The Bidder must maintain adequate insurance coverage throughout the contract period including:

- Cyber Insurance: Minimum ₹50 Crores coverage per incident for first-party and third-party cyber liability.
- Professional Indemnity Insurance: Minimum ₹10 Crores per incident.
- Fidelity Bond/Employee Dishonesty Insurance covering deployed resources.
- Copies of valid insurance policies must be shared with both Banks on request.

16.15 Compliance with IT Act 2000

The equipment, application, and services to be supplied under this contract must comply with the requirements of the Information Technology (IT) Act, 2000, and all subsequent amendments, along with related Government of India/RBI guidelines issued from time to time.

16.16 Solicitation of Employees

The selected Bidder, during the term of the contract shall not without the express written consent of the Bank, directly or indirectly:

- a. recruit, hire, appoint or engage or attempt to recruit, hire, appoint or engage or discuss employment with or otherwise utilize the services of any person who has been an employee or associate or engaged in any capacity, by the Bank in rendering services in relation to the contract; or
- b. induce any person who shall have been an employee or associate of the Bank at any time to terminate his/ her relationship with the Bank.

16.17 Amalgamation of Supplier

If the Bidder undergoes a merger, acquisition, or change of control, the Banks reserve the right to review and approve the successor entity's ability to continue performance. The Bidder must notify both Banks at least 30 days before any such event. Failure to notify is a material breach of contract.

16.18 Use of Contract Documents and Information

The successful bidder shall not, without the Purchaser's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Purchaser in connection therewith, to any person other than a person employed/authorized by the successful bidder in the performance of the Contract. Disclosure to any such employed/authorized person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

The successful bidder shall not, without the Purchaser's prior written consent, make use of any document or information pertaining to this contract except for purposes of performing the Contract.

16.19 Inspections and Tests

The Purchaser or its representative(s), RBI or any of the Statutory bodies, shall have the right to visit and /or inspect any of the Bidder's premises to ensure that software / code provided to the Bank is secured or goods conform to requisite specifications.

Any charges payable to the Purchaser's representative designated for inspection shall be borne by the Purchaser.

Should any inspected or tested Goods/software fail to conform to the Specifications, the Purchaser may reject the Goods/software, and the Supplier shall make alterations necessary to meet specification requirements at no additional cost to the Purchaser.

The Purchaser's right to inspect, test and, where necessary, reject the Goods or software after the delivery shall in no way be limited or waived by reason of the goods/software having previously been inspected, tested and passed by the Purchaser.

The supplier shall provide unrestricted access to its premises and records being maintained with regard to the job being performed as per its contract with the Bank, to the authorized personnel of the Bank/ its auditors (internal and external)/ any statutory/ regulatory authority/ authorized personnel from RBI to carry out any kind of process of audit including that of its operations and records related to services provided to the Bank, in the presence of representatives of the supplier, at any point of time giving advance notice. RBI or persons authorized by it shall access the records of Bank and the supplier related to this agreement and cause inspection.

16.20 Implementation of Services

The successful bidder shall provide all the services specified hereunder having Technical and Functional specifications in accordance with the highest standards of professional competence and integrity. If the Bank finds that any of the staff of the successful bidder assigned to work at the Bank's site is not responsive, then the successful bidder will be notified accordingly and the successful bidder shall be under obligation to resolve the issue expeditiously to the satisfaction of the Bank.

16.21 Termination for Insolvency

If the successful bidder becomes bankrupt or insolvent, has a receiving order issued against it, compounds with its creditors, or, if the successful bidder is a corporation, a resolution is passed or order is made for its winding up (other than a voluntary liquidation for the purposes of amalgamation or reconstruction), a receiver is appointed over in part of its undertaking or assets, or if the successful bidder takes or suffers any other analogous action in consequence of a debt; then the Bank may at any time terminate the contract by giving a notice to the successful bidder.

If the contract is terminated by the Bank in terms of this clause, termination will be without compensation to the successful bidder provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Bank.

In case the termination occurs before implementation of the project/ delivery of goods/services in full, in terms of this clause, the Bank is entitled to make its claim to the extent of the amount already paid by the Bank to the successful bidder.

16.22 Compliance with Statutory and Regulatory Provisions

The successful bidder shall comply without any extra cost to bank with all statutory and Regulatory provisions while executing the contract awarded by Bank.

16.23 Compliance with Policy

The successful bidder shall have to comply without any extra cost to bank with Uttar Pradesh Gramin Bank's policies like IT policy, Information Security policy, Cyber Security Policy, Digital Personal Data Protection Policy etc. in key concern areas relevant to the RFP, details of which shall be shared with the successful bidder.

16.24 Other Terms and Conditions

The relationship between the Bank and Successful Bidder/s is on principal-to-principal basis. Nothing contained herein shall be deemed to create any association, partnership, joint venture or relationship or principal and agent or master and servant or employer and employee between the Bank and Successful Bidder/s hereto or any affiliates or subsidiaries thereof or to provide any party with the right, power or authority, whether express or implied to create any such duty or obligation

on behalf of the other party.

Successful bidder/Service Provider shall be the principal employer of the employees, agents, contractors, subcontractors etc., engaged by the successful bidder/Service Provider and shall be vicariously liable for all the acts, deeds, matters or things, of such persons whether the same is within the scope of power or outside the scope of power, vested under the contract. No right of any employment in the Bank shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc., by the successful bidder/Service Provider, for any assignment under the contract. All remuneration, claims, wages dues etc., of such employees, agents, contractors, subcontractors etc., of the successful bidder/Service Provider shall be paid by the successful bidder/Service Provider alone and the Bank shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of the successful bidder's/Service Provider's employees, agents, contractors, subcontractors etc. The Successful Bidder/Service Provider shall agree to hold the Bank, its successors, assigns and administrators fully indemnified, and harmless against loss or liability, claims, actions or proceedings, if any, whatsoever nature that may arise or caused to the Bank through the action of Successful Bidder/Service Provider's employees, agents, contractors, subcontractors etc.

16.25 General Terms and Conditions

Rejection of Bids

The Bank reserves the right to reject the Bid if,

- I. Bidder does not meet any of the pre-bid eligibility criteria mentioned above including non-payment of the bid cost.
- II. The bid is incomplete as per the RFP requirements.
- III. Any condition stated by the bidder is not acceptable to the Bank.
- IV. If the RFP and any of the terms and conditions stipulated in the document are not accepted by the authorized representatives of the bidder.
- V. Required information not submitted as per the format given.
- VI. Any information submitted by the bidder is found to be untrue/fake/false.
- VII. The bidder does not provide, within the time specified by the bank, the supplemental information / clarification sought by the bank for evaluation of bid.
- VIII. The Bank shall be under no obligation to accept any offer received in response to this RFP and shall be entitled to reject any or all offers without assigning any reason whatsoever. The Bank may abort entire process at any stage without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for Bank's action.
- IX. In order to promote consistency among the Proposals and to minimize potential misunderstandings regarding how Proposals will be interpreted by the Bank, the format in which Bidders will specify the fundamental aspects of their Proposals has been broadly outlined in this RFP.
- X. Any clarifications to the RFP should be sought by email as per the dates mentioned in "Schedule [A] Important Dates". Bank will hold a pre-bid meeting, to answer all the questions / queries received by email which would also be uploaded on bank's website and GeM portal.
- XI. Proposals received by the Bank after the specified time and date shall not be eligible for consideration and shall be summarily rejected.
- XII. In case of any change in timeline, the same shall be updated on the Bank's website and shall be applicable uniformly to all bidders.

16.26 No Right to Set Off

In case the Successful Bidder has any other business relationship with the Bank, no right of set-off, counter-claim and cross-claim and or otherwise will be available under the agreement to the said Bidder for any payments receivable under and in accordance with that business.

16.27 Notices and Other Communication

If a notice has to be sent to either of the parties following the signing of the contract, it has to be in writing and shall be sent personally or by certified or registered post with acknowledgement due or overnight courier or email duly transmitted, addressed to the other party at the addresses, email

given in the contract.

Notices shall be deemed given upon receipt, except that notices sent by registered post in a correctly addressed envelope shall be deemed to be delivered within 5 working days (excluding Sundays and public holidays) after the date of mailing dispatch and in case the communication is made by email, on business date immediately after the date of successful email. (that is, the sender has a hard copy of the page evidencing that the email sent to correct email address).

Any Party may change the address, email address and fax number to which notices are to be sent to it, by providing written notice to the other Party in one of the manners provided in this section.

16.28 Substitutions of Team Members

The BID should also contain resource planning proposed to be deployed for the project which includes inter-alia, the number of personnel, skill profile of each personnel, duration of employment etc.

During the assignment, the substitution of key staff identified for the assignment shall not be allowed unless such substitution becomes unavoidable to overcome the undue delay or that such changes are critical to meet the obligation. In such circumstances, the Bidder can do so only with the concurrence of the Bank by providing alternate staff of same level of qualifications and expertise. If the Bank is not satisfied with the substitution, the Bank reserves the right to terminate the contract and recover whatever payments has been made by the Bank to the Bidder during the course of this assignment besides claiming an amount, equal to 10% of the contract value as liquidated damages. The Bank reserves the right to insist the Bidder to replace any team member with another (with the qualifications and expertise as required by the Bank) during the course of assignment. The Bidder will have to undertake that no such substitution would delay the project timelines.

16.29 Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this RFP shall not be affected or impaired.

16.30 Publicity

Any publicity by the Bidder in which the name of the Bank is to be used should be done only with the explicit written permission of the Bank.

16.31 Taxes and Duties

The successful bidder shall be liable to pay all taxes that shall be levied against it, in accordance with the laws applicable from time to time in India.

16.32 Coverage of Successful Bidder under the Employee's Provident Funds and Miscellaneous Provisions Act, 1952

The Successful bidder must submit necessary details of all the outsourced employees for any type of services engaged either through contractors or directly whenever required by the Bank. If engaged through contractors, list of all the contractors engaged for any/all services and whether the said contractors are covered independently under the EPF & MP Act 1952 is to be submitted on the Bank's request. The agreement of contracts with the contractors, the PF code number of the contractors, if covered, the attendance of the contract employees, the remitted PF challan with the Electronic Challan cum Return (ECR) should be submitted on the Bank's request.

16.33 Disclaimer

Both Bank and/or its officers, employees disown all liabilities or claims arising out of any loss or damage, whether foreseeable or not, suffered by any person acting on or refraining from acting because of any information including statements, information, forecasts, estimates or projections contained in this document or conduct ancillary to it whether or not the loss or damage arises in

connection with any omission, negligence, default, lack of care or misrepresentation on the part of Bank and/or any of its officers, employees.

This RFP is not an agreement by the Authority to the prospective Bidders or any other person. The Bank shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

The information contained in this RFP document, or any information provided subsequently to Bidder(s) whether verbally or in documentary form by or on behalf of 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 Bank to the interested parties 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. This RFP does not claim to contain all the information each bidder may require. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary, obtain independent advice. 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.

16.34 Acceptance of Purchase Order

Acceptance of purchase order should be submitted within 15 days of issuance of purchase order along-with authorization letter by the successful bidder to the Bank. If for any reason successful bidder backs out after issuance of purchase order or the purchase order issued to the successful bidder does not get executed in part / full, Bank shall invoke performance bank guarantee and blacklist the bidder for a period of two year with reporting to appropriate authorities.

16.35 Patent Rights

The Supplier shall indemnify the Bank against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods or software or hardware or any part thereof. In the event of any claim asserted by the third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the Goods or any part thereof, the bidder shall act expeditiously to extinguish such claims. If the bidder fails to comply and Bank is required to pay compensation to a third party resulting from such infringement, the bidder shall be responsible for the compensation including all expenses, court costs and lawyer fees. Bank will give notice to the bidder of such claims, if it is made, without delay by e-mail/registered post.

16.36 Bank's right to Accept or Reject any Bid or all Bids

Both Banks reserves the right to accept or reject any bid / all bids or annul the bidding process at any time prior to awarding the contract, without thereby incurring any liability to the affected Bidder or Bidders.

Both Bank reserves the right to modify the terms and conditions of this RFP duly informing the same before due date of submission of bids & publishing the same on Bank Website and GeM portal.

16.37 Liquidated Damages

The Bank will consider the inability of the successful bidder to deliver the manpower and other deliverables as per scope of this RFP and proposed Agreement within the specified time limit, as a breach of Contract and would entail the payment of penalty on the part of the successful bidder. The penalty and liquidated damages represent an estimate of the loss or damage that the Bank may have suffered due to delay in performance of the obligations (relating to delivery, implementation and Training etc.) by the successful bidder.

If Successful bidders fail to deliver any or all of the Service(s) / Systems or perform the Services within the time period(s) specified in the RFP/Contract / Agreement, bank shall, without prejudice to its other rights and remedies under and in accordance with the RFP/Contract / Agreement, levy

Liquidated Damages (LD) from payments, which are due to the Successful bidder.

For calculation of LD:

LD for delay in the Service(s) rendered for each week of delay beyond the scheduled date or part thereof will be a sum equivalent to 0.1 % of total cost of the project or TCO per week. In case of undue delay beyond a period of 15 days after attaining the maximum penalty of 10% of total project cost or TCO during implementation, Bank may consider termination of the contract or purchase order.

- The contract price for calculation of LD is TCO.
- The overall LD during implementation will be to a maximum of 10% of the total cost of the project excluding ATS
- The Bank reserves its right to recover these amounts by any mode such as adjusting from any payments to be made by the Bank to the Bidder under this contract.
- Part of week will be treated as a week for this purpose.
- However, the Bank may, at its discretion, waive the liquidated damages in case the delay cannot be attributed to the Bidder.
- Bank will deduct the amount of liquidated damages from the payment due of the same project from the Successful bidder. Bank may also withhold the amount to be recovered from the payment due from other projects held by the same bidder.
- Any such recovery or liquidated damages shall not in any way relieve the Successful bidder from any of its obligations to complete the works / service(s) or from any other obligations and liabilities under the Contract/Agreement/ Purchase Order.
- Both the above penalty as well as liquidated damages are independent of each other and are applicable separately and concurrently in addition to the termination of the contract if found desirable by the Bank.

17. Bidder Grievance Redressal Mechanism

17.1 Designated Officers for Receipt of Grievances

Any bidder aggrieved by any action, omission, decision, or outcome during the procurement process may submit its grievance/representation in writing to the designated officers of both Banks as under:

For UPGB:

General Manager, Fraud Risk Management Department
Uttar Pradesh Gramin Bank
Head Office, Lucknow
Email: frmc.ho@upgb.bank.in

For GGB:

General Manager, Risk Management Department
Gujarat Gramin Bank
Head Office, Vadodara
Email: riskmanagement.ho@ggb.bank.in

17.2 Time Limit for Submission of Representation

Any aggrieved bidder may submit a written representation/grievance to the designated officers within five (5) working days from the date of occurrence of the event giving rise to the grievance or from the date of communication/publication of the decision, whichever is applicable. Representations received after the stipulated period may not be entertained.

17.3 Disposal of Grievances

The Joint Evaluation Committee/Competent Authority of the Banks shall examine the grievance and communicate its decision to the bidder within fifteen (15) working days from the date of receipt of the representation. The decision of the Banks in this regard shall be final and binding on all bidders.

17.4 Debriefing of Bidders

After completion of the technical and/or commercial evaluation process, an unsuccessful bidder may seek a debriefing regarding its evaluation results by submitting a written request to the designated officers within five (5) working days from the date of communication of the evaluation outcome.

The Banks may, at their discretion, provide a debriefing limited to the bidder's own technical/commercial evaluation results, strengths, and deficiencies. Information relating to other bidders, comparative rankings, proprietary information, trade secrets, or details affecting confidentiality and competitive neutrality shall not be disclosed.

17.5 No Stay on Procurement Process

Submission of a grievance or request for debriefing shall not entitle the bidder to any stay, suspension, or postponement of the procurement process, and the Banks reserve the right to proceed with the tender process in accordance with the RFP.

SECTION – IV: BID SUBMISSION INSTRUCTIONS

1. Submission via GeM Portal

All bid documents must be submitted online through the Government e-Marketplace (GeM) portal (www.gem.gov.in) as part of the e-Procurement process. Bidders must register on GeM before participating. The following documents are to be uploaded online as part of the bid:

- Eligibility Criteria compliance along with all supporting documents.
- All Annexures as per this RFP on Bidder's letterhead with authorised signatory's signature and company seal on all pages.
- All supporting documents and product literature for Technical/Functional Specifications.
- Relevant brochures and marketing materials.
- Compliance to Technical/Functional Specifications as per Annexure-XV.
- Commercial Bid as per Part-II of Section-V
- SBOM (Software Bill of Materials).
- Any other information requested by either Bank in relation to this tender.

Documents must be in searchable PDF format (OCR-enabled). Bidders must ensure files are named clearly and are fully legible. Bidders are responsible for ensuring all uploaded files are valid and not corrupt. Technical glitches during last-minute submissions are not grounds for deadline extension.

2. Offline Physical Submissions (to both Banks)

In addition to GeM online submission, Bidders must submit the following physically in sealed envelopes to BOTH Banks by the deadline:

- Joint Bid Security (EMD) – Single Bank Guarantee of ₹60,00,000/- naming both UPGB and GGB as co-beneficiaries.
- Pre-Contract Integrity Pact (Annexure-V) duly signed on stamp paper by Authorised Signatory.

Envelopes must be super-scribed: "Joint RFP for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management Solution – DO NOT OPEN BEFORE [DATE AND TIME OF TECHNICAL BID OPENING]". Name and address of Bidder must be clearly written on the envelope.

3. Instructions for Bid Submission

- All pages of the bid must be initialled by the Authorised Signatory with company seal.
- Bid form must be signed in full with official seal.
- Any interlineation, erasure, or overwriting must be initialled by the Authorised Signatory.
- No column in any prescribed format shall be left blank. Blank entries will be treated as non-compliant.
- Price information must NOT be submitted with Technical Bid. Technical bids containing price information will be summarily rejected.
- Bids submitted by any mode other than GeM (except offline documents) will not be accepted.

4. Two-Part Bid Structure

- Part-I (Technical Bid): Complete compliance details, eligibility documents, technical specifications compliance, all Annexures except Commercial Bid.
- Part-II (Commercial Bid): Bank-wise pricing as per the Commercial Bid format (Annexure-XVI). Submitted online via GeM simultaneously with Technical Bid but opened only after Stage 2 qualification.

5. Key Instructions for Bidders

1. Register on GeM portal well in advance of the bid submission deadline.
2. Get your organisation's executives trained on GeM portal operations before submission.
3. Submit bids well in advance of the deadline to avoid last-minute technical issues.
4. Submit offline documents (EMD and Integrity Pact) to both Banks simultaneously.
5. Ensure all claimed capabilities are demonstrable during product presentation/demo.

SECTION – V: TECHNICAL AND COMMERCIAL BID

PART – I: TECHNICAL AND FUNCTIONAL COMPLIANCE MATRIX

Date:

The General Manager
Fraud Risk Management, Cell
2nd Floor, Uttar Pradesh Gramin Bank
Head Office, NBCC Building
Vardan Khand, Gomti Nagar Ext, Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

Referring to your above RFP, we submit the compliance details of the specifications given below:

TECHNICAL/ FUNCTIONAL SPECIFICATIONS:

The detailed functional / technical requirement with marking scheme for each of the feature is as follows:

Refer Functional Specification and Technical Specification mentioned under scope of work (attached Functional Specification and Technical Specification submission format provided in separate [Annexure-XV](#), Items which will be customised before project Go live to be specified as per [Annexure- XVI](#)) along with the required hardware sizing documents specified in [Annexure-XXIII](#)

We comply with all requirements, specifications, terms and conditions mentioned in the Bid Document. We agree for the time frame for completion of activities as per your above bid.

We agree to the terms of payment mentioned in your bid.

We submit that we shall abide by your terms and conditions governing the quotation. We submit that the details given above are true to the best of our knowledge.

For

Office Seal

(Authorised Signatory)

Place:

Name:

Date:

Designation: Mobile No:

Business Address: Telephone No:

E-mail ID:

PART – II: COMMERCIAL BID FORMAT

(Price Bid to be submitted online via GeM portal along with Technical Bid, opened only after Stage 2 qualification)

To, The General Manager, Joint EFRM RFP Committee, Uttar Pradesh Gramin Bank / Gujarat Gramin Bank
 Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (EFRM) Solution for UPGB and GGB.

Commercial Table – Summary of Cost

S.No.	Item	Ref. Table	Cost (INR)	GST %	GST Amount (INR)	Total (incl. GST)
1	Enterprise License Fee (EFRMS) incl. 1 Year Warranty at DC & DR	A				
2	Annual Maintenance Contract (AMC) Cost for 4 years	A				
3	Installation, Implementation, Configuration, and Integration Cost	B				
4	Onsite Technical Support (OTS/FMS) Cost (5 years)	C				
5	Change Request / Enhancement Cost (per person-day rate)	D				
	TOTAL COST OF OWNERSHIP (TCO) = A+B+C		[TCO]			Combined TCO
	Total Cost in Words : Rupees ...					

NOTE: Year 1 will start after Phase 2 Go-Live for each Bank independently. License cost in any year must not exceed 30% nor be less than 15% of overall Total Table-A cost. ATS/AMC per annum: 10%–15% of capital cost.

Table – A: Enterprise License and AMC Cost

S.No.	Items	Year 1*	Year 2	Year 3	Year 4	Year 5	Total
1	Enterprise License Fee (all channels, all transactions, all users) incl. 1 Year Warranty*						
2	Annual Maintenance Contract (AMC) – 4 years post warranty	N/A					

S.No.	Items	Year 1*	Year 2	Year 3	Year 4	Year 5	Total
	GST Amount						
	TOTAL TABLE-A						

Table – B: Implementation, Integration, and Configuration Cost

S.No.	Description	Cost
B.1	UPI (Inward & Outward)	
B.2	Mobile Banking with Step-Up Authentication	
B.3	Internet Banking with Step-Up Authentication	
B.4	Debit Card (ATM Switch) including POS and E-Commerce	
B.5	IMPS (Inward & Outward)	
B.6	AEPS (Aadhaar Enabled Payment System)	
B.7	NEFT & RTGS (Inward & Outward)	
B.8	Call Centre & IVRS Integration	
B.9	CBS / Branch Transactions (Finacle) including Staff, Internal, Money Mule monitoring Sub-Total Phase 2	
B.10	BBPS (Inward & Outward)	
B.11	SMS Gateway (2FA, OTP, TOTP, Risk-based alerts)	
B.12	Behavioural Biometric Application Integration (Android, iOS, JS SDKs)	
B.13	Email Gateway	
B.14	<ul style="list-style-type: none"> • Payment Gateway / Payment Aggregators, Government Business Transactions, PFMS • NPCI EFRMS (National Payments Corporation of India EFRM System feeds) • Any additional channels deployed by either Bank during the contract period External Threat Intelligence Feeds: Neustar, Maxmind, Lexis Nexis, Group-IB, RSA, I4C Suspect Registry, CFR, CIBIL, CRILC, ECGC, DIP, and others as required	
B.15	<ul style="list-style-type: none"> • HRMS 	
B.16	<ul style="list-style-type: none"> • AML Solution 	

S.No.	Description	Cost
	Sub-Total Phase 3	
	TOTAL TABLE-B	

Table – C: Onsite Technical Support (OTS/FMS) Cost

S.No.	Resource Level	Count	Annual Cost	5-Year Total
C.1	L1 Support Engineer (24x7x365 onsite per Bank)			
C.2	L2 Support Engineer (Business hours + on-call)			
C.3	L3 Support Engineer (Onsite for critical; remote otherwise)			
	TOTAL TABLE-C			

Table – D: Change Request / Enhancement Pricing

S.No.	Role	Rate per Person-Day (INR)
D.1	Change request cost	

NOTE: Change Request rates are applicable for customisations beyond the 500 annual rule and 30 models (for each bank separately) customisations included under ATS. RBI/NABARD-mandated changes are always free of cost. Change Request rates are fixed for the contract period.

We comply with all requirements, specifications, terms and conditions mentioned in this Joint Bid Document. We agree to the timeframes for completion of activities as per this Bid. We agree to the terms of payment mentioned in this Bid. We submit that the details given above are true to the best of our knowledge.

Office Seal	Authorised Signatory	Name:	Designation:
Place:	Date:	Mobile No.:	Email ID:

Notes:

- These details should be on the letter head of Bidder and each & every page should be signed by an Authorized Signatory with Name and Seal of the Company.
- The rate quoted shall be inclusive of Taxes. Applicable GST shall be paid by the Bank at actual prevailing rate.
- No counter condition/assumption in response to Commercial Bid will be accepted. Bank has a right to reject such bid.
- Bidders are required to include all cost for the entire project period as Bank would not be paying anything extra over above quoted rate.
- Billing will be done at the end of the quarter.

Price Composition and Total Cost of Ownership (TCO):

- The price quoted should be in Indian rupees only.
- Above quoted total cost will be utilized for calculation of Techno - commercial evaluation for finalizing H1 vendor.
- The cost needs to include all services and other requirement as mentioned in the RFP.
- All Quoted Commercial Values should comprise of values only up to 2 decimal places. Bank for evaluation purpose will consider values only up to 2 decimal places for all calculations & ignore all figures beyond 2 decimal places.
- For each of the above items provided, bidder is required to provide the cost for every line item where the bidder has considered the cost.
- All the commercial value should be quoted in Indian Rupees & shall be all inclusive of taxes excluding GST. GST will be paid extra as per actuals. The Bidder is expected to provide the GST amount and GST percentage in commercial Bid (without amounts being submitted in the technical response). There will be no price escalation for during the contract period and any extension thereof in the contract. Bid submitted with an adjustable price quotation will be treated as non-responsive and will be rejected.
- If the cost for any line item is indicated as zero, then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
- All deliverables to be supplied as per tender requirements provided in the tender.
- The bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations.
- Bank will deduct applicable TDS, if any, as per the law of the land.

TCO shall encompass but not be limited to the following:

- Cost of the Software and Technology
- License fee (Corporate or user specific)
- Installation, commissioning and integration charges, if any.
- Master Service Agreement/Service Level Agreement (SLA) costs as per applicable stamp duty/other fees for applicable period.
- Any cost towards development of interface and/or customization to meet Bank's requirement/communicating with the Bank's core banking solution, intermediary server etc. Cost of system/software up gradation for the entire period of contract.
- Any other cost expected by vendor for timely and efficient implementation of the project as per business requirement.
- Cost of integration with our system (APIs etc. for integration with Bank's CBS system Banc slink, Middleware etc.) Vendor will have to adhere to Bank's existing format interface specification.
- Installation and commissioning charges, training to Bank staff.
- Integration with system vendors used by the bank.

LIST OF ANNEXURES

Annexure	Title	Submitted By	Format
Annexure-I	Bid Form / Letter of Acceptance	Bidder	Letterhead
Annexure-II	Self-Declaration – Blacklisting / Debarment	Bidder	Letterhead
Annexure-III	Contract Form (Draft)	Both Banks	Bank Template
Annexure-IV	Performance Bank Guarantee Format	Bidder / Banker	Bank Template
Annexure-V	Pre-Contract Integrity Pact	Bidder	Stamp Paper
Annexure-VI	Non-Disclosure Agreement (NDA)	Bidder	Bank Template
Annexure-VII	Declaration for MSE Benefits (if applicable)	Bidder	Letterhead
Annexure-VIII	Declaration on Procurement from Border Country Bidder	Bidder	Letterhead
Annexure-IX	Declaration of Source Code Audit	Bidder/OEM	Letterhead
Annexure-X	Checklist for RFP Document Completeness	Bidder	Bank Template
Annexure-XI	Pre-Bid Query Format	Bidder	Excel/Bank Template
Annexure-XII	Experience Details / Reference Site Summary	Bidder/OEM	Bank Template
Annexure-XIII	Turnover, Net Worth and P&L Certificate	CA/Statutory Auditor	Letterhead
Annexure-XIV	Bid Security Form (EMD) / Bid Security Declaration	Bidder/Banker	Bank Template
Annexure-XV	Functional and Technical Compliance Matrix	Bidder	Bank Template
Annexure-XVI	Commercial Bid Format (Tables A, B, C, D – Bank-wise)	Bidder	Bank Template
Annexure-XVII	Labour Law Compliance Certificate	CA/Auditor or Bidder	Letterhead
Annexure-XVIII	Authorisation Letter (Power of Attorney)	Bidder	Stamp Paper
Annexure-XIX	Manufacturers' Authorisation Form (MAF)	OEM	OEM Letterhead
Annexure-XX	Undertaking for Being OEM of Proposed Product	OEM/Bidder	Letterhead

Annexure	Title	Submitted By	Format
Annexure-XXI	Reference Site Details (per Qualifying Bank)	Bidder/OEM	Bank Template
Annexure-XXII	Know Your Employee (KYE) Clause Undertaking	Bidder	Letterhead
Annexure-XXIII	Hardware Requirements (Sizing per Bank: DC, DR, UAT)	Bidder	Bank Template
Annexure-XXIV	Work Experience Certificate (from Reference Banks)	Reference Bank	Bank Letterhead
Annexure-XXV	Undertaking for Product Presentation and Implementation Readiness	Bidder/OEM	Letterhead
Annexure-XXVI	Details of Hardware, OS and DB Requirements	Bidder	Bank Template
Annexure-XXVII	Data Security and Segregation Compliance Undertaking	Bidder	Bank Template

ANNEXURE-I Bid Form/Letter of Acceptance

(Bidders are required to furnish the Bid Form on its letter head)

Date:

To

The General Manager
Fraud Risk Management Department,
2nd Floor, Uttar Pradesh Gramin Bank, Head Office, NBCC Building
Vardan Khand, Gomti Nagar Ext, Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

Having examined the Bidding Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to..... (Description of Goods and Services), in conformity with the said Bidding Documents.

We undertake, if our bid is accepted, to deliver the goods & services in accordance with the delivery schedule specified in the Schedule of Requirements.

If our bid is accepted, we will obtain the Guarantee of a Bank in a sum equivalent to 5% per cent of the Contract Price for the due performance of the Contract, in the form prescribed by the Bank. We agree to abide by this for the bid validity period specified and it shall remain binding upon us and may be accepted at any time before the expiration of that period. We agree to extend the Bid Validity Period, if required.

Until a formal contract is prepared and executed, this bid, together with your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India.

We understand that you are not bound to accept the lowest or any bid you may receive.

We confirm that we comply with the qualification criteria of the bidding documents and are submitting proof of the same along with bid.

Dated thisday of..... 2026

Signature

.....

(In the Capacity of)

Duly authorised to sign bid for and on behalf of (Name & Address of Bidder)

.....
Mobile: Email

ANNEXURE-II Self-Declaration – Blacklisting/Debarment

The General Manager
Fraud Risk Management Department,
2nd Floor, Uttar Pradesh Gramin Bank
Head Office, NBCC Building
Vardan Khand, Gomti Nagar Ext, Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

We hereby certify that we have not been blacklisted or debarred by any Government Department / PSU / Bank / PSB / Financial Institution at the time of submission of bid and Bidder not insolvent, bankrupt, in receivership, or being wound up..

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE–III Contract Form (Draft)

(To be submitted on Non - Judicial Stamp Paper)

THIS AGREEMENT made theday of2026, Between Uttar Pradesh Gramin Bank/ Gujrat Gramin Bank, having its Head Office, 2nd and 3rd Floor, NBCC Building, Vardan Khand, Gomti Nagar Ext Extention, Luknow-226010 (hereinafter “the Purchaser”) which term shall unless repugnant to the context or meaning thereof shall mean its successors and assigns) of the one part and(Name of Supplier) having its Registered Office at (City and Country of Supplier) (hereinafter called “the Supplier”) which term shall unless repugnant to the context or meaning thereof shall mean its successors and permitted assigns) of the other part:

WHEREAS the Purchaser invited bids vide RFP No. for certain Goods and ancillary services viz., (Brief Description of Goods and Services) and has accepted a bid by the Supplier for the provision of those goods and services in the sum for (Contract Price in Words and Figures) (hereinafter called “the Contract Price”). NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.
2. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:
 - (a) the Bid Form and the Price Schedule submitted by the Bidder;
 - (b) the Schedule of Requirements.
 - (c) the Functional & Technical Specifications;
 - (d) the Conditions of Contract;
 - (e) the Purchaser’s Notification of Award/Purchase Order.
 - (f) the RFP including Addendum/s & corrigendum/s.
3. In consideration of the payments to be made by the Purchaser to the Supplier as hereinafter mentioned, the Supplier hereby covenants with the Purchaser to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the Contract.
4. The Purchaser hereby covenants to pay the Supplier in consideration of the provision of the goods and services and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

Brief particulars of the goods and services which shall be supplied/provided by the Supplier are as under:

S l . N o .	Brief description of goods & services	Quantity to be supplied	Un it pri ce	Tot al pric e

TOTAL VALUE:

DELIVERY SCHEDULE:

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

Signed, Sealed and Delivered by the
said..... (For Uttar Pradesh Gramin Bank)
in the presence of:

Signed, Sealed and Delivered by the
said..... (For the supplier)
in the presence of:.....

ANNEXURE-IV Performance Bank Guarantee Format

Bank Guarantee No.

Date:

To:
The General Manager
Fraud Risk Management Department
2nd and 3rd Floor, Uttar Pradesh
Gramin Bank
Head Office, NBCC Building, Vardan Khand
Gomti Nager Ext, Lucknow-226010

WHEREAS..... (Name of Supplier) hereinafter called "the Supplier") has undertaken, in pursuance. of Contract No..... dated to.....(Description of Goods and Services) (hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with the Supplier's performance obligations in accordance with the Contract including Maintenance and Repairs of the entire system including cost of spares during warranty period. AND WHEREAS we have agreed to issue a Guarantee in your favour on the request of the Supplier:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total sum of Rs..... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without any demur, cavil or protest, any sum or sums within the limit of (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein. This guarantee is valid until theday of.....20__

Signature of Authorized Official with Seal

Date..... 202...
Address:

NOTE:

1. Supplier should ensure that seal and code no of the signatory is put by the bankers, before submission of the bank guarantee.
2. Bank Guarantee issued by a scheduled commercial Banks located in India and shall be on a Non- Judicial Stamp Paper of requisite value.

ANNEXURE-V - Pre-Contract Integrity Pact

(To be submitted on Non - Judicial Stamp Paper)

PRE-CONTRACT INTEGRITY PACT

Between

Uttar Pradesh Gramin Bank / Gujrat Gramin Bank

hereinafter referred to as "The Bank" and

.....hereinafter referred to as "The Bidder/Contractor"

Preamble

The Bank intends to award, under laid down organizational procedures, contract/s for **Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution**. The Bank values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder(s) and / or Contractor(s).

In order to achieve these goals, the Bank will appoint an Independent External Monitor/s (IEM), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1 – Commitments of the Bank

The Bank commits itself to take all measures necessary to prevent corruption and to observe the following principles:

No employee of the Bank, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

The Bank will, during the tender process treat all Bidder(s) with equity and reason. The Bank will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

The Bank will exclude from the process all known prejudiced persons.

If the Bank obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act, or if there be a substantive suspicion in this regard, the Bank will inform the Chief Vigilance Officer (CVO) and in addition can initiate disciplinary actions.

Section 2 – Commitment of the Bidder(s)/ Contractor(s)

1. The Bidder(s) / Contractor(s) commit themselves to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

The Bidder(s) / Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the Bank's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

The Bidder(s) / Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

The Bidder(s) / Contractor(s) will not commit any offence under the relevant IPC/PC Act: further, the Bidder (s) / Contractor (s) will not use improperly, for purpose of competition or personal gain, or pass on to others, any information or documents provided by the Bank as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

The Bidder (s) / Contractor (s) of foreign origin shall disclose the name and address of the Agents/Representatives in India, if any. Similarly, the Bidder(s)/Contractor (s) of Indian Nationality shall furnish the name and address of the foreign principals, if any. Further, as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder (s) / Contractor (s). Further as mentioned in the Guidelines, all the payments made to the Indian Agent/Representative have to be in Indian Rupees only. Copy of the "Guidelines on Indian Agents of Foreign Suppliers" is placed at Annexure.

The Bidder (s) / Contractor (s) will, when presenting his bid, disclose any and all payments he has made, is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2. The Bidder (s) / Contractor (s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

Section 3– Disqualification from tender process and exclusion from future contracts

If the Bidder(s) / Contractor(s), before award or during execution has committed a transgression through a violation of Section 2, above or any other form such as to put his reliability or creditability in question, the Bank is entitled to disqualify the Bidder(s) / Contractor(s) from the tender process.

Section 4 – Compensation for Damages

If the Bank has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Bank is entitled to demand and recover the damages equivalent to Bid Security and this bid security will be forfeited.

If the Bank has terminated the contract according to Section 3, or if the Bank is entitled to terminate the contract according to Section 3, the Bank shall be entitled to demand and recover from the Contractor the liquidated damages equivalent to the amount of the contract value.

Section 5 – Previous Transgression

The Bidders declares that no previous transgressions occurred in the last three years with any other Company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprises in India that could justify his exclusion from the tender process.

The Bidder agrees that if he makes incorrect statement on this subject, bidder is liable to be disqualified from the tender process or the contract, if already awarded, is liable to be terminated for such reason. The imposition and duration of the execution of the bidder will be determined by the bidder based on the severity of transgression.

The Bidder/Contractor acknowledges and undertakes to respect and uphold the Bank absolute right to resort to and impose such exclusion.

Apart from the above, the Bank may take action for banning of business dealings/holiday listing of the Bidder/ Contractor as deemed fit by the Bank.

If the Bidder/Contractor can prove that he has resorted/recouped the damage caused by him and has implemented a suitable corruption prevention system, the Bank may, at its own discretion, as per laid down organizational procedures, revoke the exclusion prematurely.

Section 6 – Equal treatment of all Bidders/ Contractors/ Sub-Contractors

The Bidder(s)/Contractor(s) undertake(s) to demand from all sub-contractors a commitment in conformity with this Pre-Contract Integrity Pact, and to submit it to the Bank before contract signing. The Bidder(s)/Contractor(s) shall be responsible for any violation(s) of the principles laid down in this agreement/Pact by any of its Sub-contractors/Sub-vendors.

The Bank will enter into agreement with identical conditions as this one with all Bidders/Contractors. The Bank will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 – Criminal charges against violating Bidder(s) /Contractor(s) /Sub contractor(s)

If the Bank obtains knowledge of conduct of a Bidder, Contractor or Sub-contractor or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or of the Bank has substantive suspicion in this regard, the Bank will inform the same to the Chief Vigilance Officer.

Section 8 – Independent External Monitor / Monitors

The Bank appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

The Name and Contact details of the Independent External Monitor (IEM) nominated by the Bank are as under:

Shri Bishwamitra Pandey
Flat No. 1104, Tower No. KNG-001
JP Greens Wish Town Klassic Sector-134
Email Id- vishwamitram1@gmail.com

Shri Anup Kumar Nayak, IFoS (Retd.)
e-mail- anupnaya@gmail.com Email Id-
vishwamitram1@gmail.com

The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. It will be obligatory for him to treat the information and documents of the Bidders/Contractors as confidential. He reports to the Authority designated by the Bank.

The Bidder(s)/Contractor(s) accept that the Monitor has the right to access without restriction to all Project documentations of the Bank including that provided by the Contractor. The Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor is under contractual obligation to treat the information and documents of the Bidders/Contractors(s)/Subcontractors(s) with confidentiality.

The Bank will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the Bank and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

As soon as the Monitor notices, or believes to notice, a violation of this agreement, he will so inform the Management of the Bank and request the Management to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.

The Monitor will submit a written report to the Authority designated by the Bank, within 8 to 10 weeks from the date of reference or intimation to him by the Bank and, should the occasion arise submit proposals for correcting problematic situations.

If the Monitor has reported to Authority designated by the Bank, a substantiated suspicion of an offence under relevant IPC/PC Act, and the Authority designated by the Bank has not, within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance

Commissioner.

The word 'Monitor' would include both singular and plural.

Section 9 – Pact Duration

This pact begins when both parties have legally signed it. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded on whomsoever it may be.

If any claim is made/lodged during this time, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/determined by the Bank.

Section 10 – Examination of Books of Accounts

In case of any allegation of, violation of any provisions of this Pre-Contract Integrity Pact or payment of commission, the Bank or its agencies shall be entitled to examine the Books of Accounts of the Bidder and the Bidder shall provide necessary information of the relevant financial documents in English and shall extend all possible help for the purpose of such examination.

Section 11 – Other provisions

This agreement is subject to Indian Law, Place of performance and jurisdiction is the Corporate Office of the Bank, i.e. Lucknow.

Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

If the Contractor is a partnership or a Consortium, this agreement must be signed by all partners or Consortium members. In case of a Company, the Pact must be signed by a representative duly authorized by Board resolution.

Should one or several provisions of this agreement turn out to be invalid, the reminder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

In the event of any contradiction between the Pre-Contract Integrity Pact and its Annexure, the Clause in the Pre-Contract Integrity Pact will prevail.

Parties signing this Pact shall not approach the courts while representing the matters to Independent External Monitors and he/she will await their decision in the matter.

Any dispute or difference arising between the parties with regard to the terms of this Agreement/Pact, any action taken by the Bank in accordance with this Agreement/Pact or interpretation thereof shall not be subject to arbitration.

The parties hereby sign this Pre-Contract Integrity Pact aton
.....

(For & On behalf of the Bank)

(For & On behalf of Bidder/Contractor)

(Office Seal)

(Office Seal)

Place _____

Place _____

Date _____

Date _____

Witness 1:

Witness 1:

(Name & Address) _____

(Name & Address) _____

Witness 2:

(Name & Address) _____

Witness 2:

(Name & Address) _____

ANNEXURE-VI Non-Disclosure Agreement (NDA)

THIS AGREEMENT made and entered into aton this theday of.....202... between Uttar Pradesh Gramin Bank, a body corporate constituted under the Banking Companies (Acquisition & Transfer of Undertakings) Act 1970, having its Corporate Office, 2nd and 3rd Floor, NBCC Building, Vardan Khand, Gomti Nagar Ext Extension, Lucknow-226010, hereinafter called the "BANK" which term shall wherever the context so require includes its successors and assigns

AND

M/s..... Limited a company registered under the Companies Act having its registered office at..... hereinafter called the "Supplier" which term shall wherever the context so require includes its successors and assigns, WITNESSETH:

WHEREAS

The Bank is inter-alia engaged in the business of banking and intends to procure **Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution**. M/s..... Limited has been engaged in the business of providing **Enterprise Fraud Risk Management solution**.

The parties have entered into agreement dated _____ for **Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution** (herein after referred to as "purpose") and have established business relationship between themselves. In course of the said purpose, it is anticipated that each party may disclose or deliver to the other certain or some of its trade secrets or confidential or proprietary information. The parties have agreed that disclosure and use of such confidential information shall be made and on the terms and conditions of this agreement.

NOW THEREFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and between the parties hereto as follows:

1. Confidential information

Confidential Information means all information disclosed/ furnished by either party to another party in connection with the Purpose. Confidential Information shall include customer data, any copy, abstract, extract, sample, note or module thereof and all electronic material or records, tenders and other written, printed or tangible thereof and include all information or material that has or could have commercial value or other utility in the business in which disclosing party is engaged.

Receiving party may use the information solely for and in connection with the Purpose.

2. Use of Confidential Information

Each party agrees not to use the other's confidential information for any purpose other than for the specific purpose. Any other use of such confidential information by any party shall be made only upon the prior written consent from the authorized representative of the other party or pursuant to subsequent agreement between the Parties hereto.

The receiving party shall not commercially use or disclose for commercial purpose any confidential information or any materials derived there from, to any other person or entity other than persons in the direct employment of the Receiving Party who have a need to access to and knowledge of the confidential information solely for the purpose authorized above. Whenever, it is expedient under the contract, the Receiving Party may disclose confidential information to consultants/third party only if the consultant/ third party has executed non-disclosure agreement with the Receiving Party that contains terms and conditions that are no less restrictive than these and such consultant should also be liable to the original disclosing party for any unauthorized use or disclosure. The Receiving party shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. The Receiving Party agrees to notify the Disclosing Party immediately if it learns of any use or disclosure of the Disclosing party's confidential information in violation of the terms of this Agreement.

Neither party shall make news release, public announcements, give interviews, issue or publish advertisements or Agreement, the contents/provisions thereof, other information relating to

Joint RFP for EFRM solution for UPGB and GGB

this

agreement, the purpose, the Confidential information or other matter of this agreement, without the prior written approval of the other party.

Upon written request by the Bank, the Supplier shall:

- I. cease using the Confidential information,
- II. return the Confidential Information and all copies, notes or extracts thereof to the Bank within seven (7) business days of receipt of request and
- III. confirm in writing that the Receiving Party has complied with the obligations set forth in this paragraph.”

3. Exemptions

The obligations imposed upon either party herein shall not apply to information, technical data or know how whether or not designated as confidential, that:

- Is already known to the Receiving party at the time of the disclosure without an obligation of confidentiality
- Is or becomes publicly known through no unauthorized act of the Receiving party
- Is rightfully received from a third party without restriction and without breach of this agreement
- Is independently developed by the Receiving party without use of the other party's confidential information and is so documented.
- Is disclosed without similar restrictions to a third party by the Party owning the confidential information
- Is approved for release by written authorization of the disclosing party; or
- Is required to be disclosed pursuant to any applicable laws or regulations or any order of a court or a governmental body; provided, however that the Receiving party shall first have given notice to the Disclosing Party and made a reasonable effort to obtain a protective order requiring that the confidential information and / or documents so disclosed used only for the purposes for which the order was issued.

4. Term

This agreement shall be effective from the date of the execution of this agreement and shall continue till expiration or termination of this agreement due to cessation of the business relationship between the parties. Upon expiration or termination as contemplated herein the Receiving party shall immediately cease any or all disclosures or uses of confidential information and at the request of the 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, note or modules thereof.

Notwithstanding the above, the obligations of the receiving party in respect of disclosure and confidentiality shall continue to be binding and applicable without limit until such information enters the public domain.

5. Title and Proprietary rights

Notwithstanding the disclosure of any confidential information by the disclosing party to the receiving party, the disclosing party shall retain title and all intellectual property and proprietary rights in the confidential information. No License under any trademark, patent or copyright or application for same which are or thereafter may be obtained by such party is either granted or implied by the conveying of confidential information.

6. Return of confidential information

Upon written demand of the disclosing party, the receiving party shall (I) cease using the confidential information (ii) return the confidential information and all copies, abstracts, extracts, samples, note or modules thereof to the disclosing party within seven (7) days after receipt of notice and (iii) upon request of the disclosing party, certify in writing that the receiving party has complied with the obligations set forth in this paragraph.

7. Remedies

The receiving party acknowledges that if the receiving party fails to comply with any of its obligations hereunder, the disclosing party may suffer immediate, irreparable harm for which monetary damages may not be adequate. The receiving party agrees that, in addition to all other remedies provided at law or in equity, the disclosing party shall be entitled to injunctive relief hereunder.

8. Entire agreement

This agreement constitutes the entire agreement between the parties relating to the matter discussed herein and supersedes any and all prior oral discussion and/or written correspondence or agreements between the parties. This agreement may be amended or modified only with the mutual written consent of the parties. Neither this agreement nor any rights, benefits and obligations granted hereunder shall be assignable or otherwise transferable.

9. Severability

If any provision herein becomes invalid, illegal or unenforceable under any law, the validity, legality and enforceability of the remaining provisions and this agreement shall not be affected or impaired.

10. Dispute resolution mechanism

In the event of any controversy or dispute regarding the interpretation of any part of this agreement or any matter connected with, arising out of, or incidental to the arrangement incorporated in this agreement, the matter shall be referred to arbitration and the award passed in such arbitration shall be binding on the parties. The arbitral proceeding shall be governed by the provisions of Arbitration and Reconciliation Act 1996 and the place of arbitration shall be Lucknow.

Submitting to arbitration may be considered as an additional remedy and it does not preclude the parties to seek redressal/ other legal recourse.

11. Jurisdiction

Any dispute arising out of this order will be under the jurisdiction of Courts of Law in Lucknow.

12. Indemnity clause

“The receiving party should indemnify and keep indemnified, saved, defended, harmless against any loss, damage, costs etc. incurred and / or suffered by the disclosing party arising out of breach of confidentiality obligations under this agreement by the receiving party etc., officers, employees, agents or consultants.”

13. Governing laws

The provisions of this agreement shall be governed by the laws of India.

In witness whereof, the parties hereto have set their hands through their authorised signatories

BANK

M/s

ANNEXURE-VII - Declaration for MSE Benefits (if Applicable)

(To be submitted on the letter head of the bidder signed by Director/Company Secretary)

To,
The General Manager
Fraud Risk Management
Department
2nd Floor, Uttar Pradesh Gramin Bank
Head Office NBCC Building, Vardan Khand
Gomti Nagar Ext ext, Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

Dear Sir,

This has reference to our bid submitted in response to your Request for Proposal (RFP) Ref. No. RFP No. dated floated for **Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution**. We have carefully gone through the contents of the above referred RFP and hereby undertake and confirm that, as per the Govt. Of India guidelines, we are eligible to avail the following MSE benefits in response to your RFP floated, as referred above.

- 1) Relaxation in number of years the firm is in operation as specified in eligibility Criteria.
- 2) Relaxation of average annual turnover as specified in eligibility Criteria.
- 3) Relaxation in work experience as specified in eligibility Criteria.
- 4) Exemption on submission of bid security

In case, at any later stage, it is found or established that, the above undertaking is not true then the Bank may take any suitable actions against us viz. Legal action, Cancellation of Notification of Award/contract (if issued any), Blacklisting & debarment from future tender/s etc.

In case, if we withdraw or modify the Bid during the period of validity, or if we are awarded the contract and fail to sign the contract, or to submit a performance security before the deadline defined in the request for proposal, we will be suspended for the period of 1 year from participation in future RFPs of the Uttar Pradesh Gramin Bank.

Yours Sincerely

For M/s _____

Signature

Name:

Designation: Director/Company Secretary Place:

Date:

Seal & Stamp

ANNEXURE-VIII Declaration on Procurement from Border Country Bidder

(THE BIDDER SHOULD GIVE THE FOLLOWING UNDERTAKING / CERTIFICATE ON ITS LETTERHEAD)

To,
The General Manager
Fraud Risk Management
Department
2nd Floor, Uttar Pradesh Gramin
Bank Head Office NBCC Building,
Vardan Khand Gomti Nagar Ext,
Lucknow-226010

Date

Dear Sirs,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

I have read the clause regarding restriction on procurement from a bidder of a country which shares a land border with India; I certify that << **name of the firm**>> is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Evidence of valid registration by the Competent Authority shall be attached, wherever applicable.]

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE-IX Declaration of Source Code Audit

To,

Date

The General Manager
Fraud Risk Management
Department
2nd Floor, Uttar Pradesh Gramin
Bank Head Office NBCC Building,
Vardan Khand Gomti Nagar Ext,
Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No. **dated**

We declare that, the source code of the application(s) proposed, where we are the OEM of the solution, to be deployed for providing testing services has been audited by professionally competent personnel/ Information Security (IS) Auditors.

We further declare that if we become successful bidder, we will submit the proof of Source Code Audit to the Bank.

Signature of Authorized Official

Name and Designation with Office Seal

Place:

Date:

ANNEXURE-X CHECKLIST FOR THE RFP DOCUMENT COMPLETENESS

S.No.	Criterion	Documentation Required
1	The bidder must be registered in India as Company/PSU/PSE/Proprietorship/Partnership/LLP. In operation minimum 5 years as of RFP date.	Certificate of Incorporation issued by Registrar of companies and full address of the registered office along with copies of MOA/AOA or Partnership Deed along with GST registration certificate.
2	<p>The Bidder is not from such a country which shares a land border with India, in terms of the said amendments to GFR, 2017.</p> <p style="text-align: center;">(or)</p> <p>The Bidder is from such a country and has been registered with the Competent Authority i.e. the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT), as stated under Annexure to the said Office Memorandum / Order and we submit the proof of registration herewith.</p>	Undertaking on letterhead. DPIIT registration certificate if applicable. (Annexure-VIII)
3	<p>The bidder must be OEM/OSD or Authorised Indian Representative. No consortium bids. The bidder must have an average turnover of minimum Rs 12 cr during last 03 (three) financial years i.e FY'23-24, FY'24-25 and FY'25-26.</p> <p>For MSEs/Startups (as per above point 6.4) an average turnover of minimum Rs. 6 Cr during last 03 (three) financial years i.e. FY 23-24, FY 24-25 and FY 25-26.</p> <p>If financial statements for 2025-26 is unaudited, the bidder can submit audited financial statements of 2022-23, 2023-24 & 2024-25 along with letter of undertaking that FY 2025-26 statement is not audited.</p>	<p>In case of authorized representative / partner of the primary product, MAF from OEM as per Annexure-XIX in their letter Head needs to be provided. (Name, designation, contact no & official mail id of the signing authority must be clearly mentioned in the MAF.)</p> <p>In case bidder itself is OEM of the EFRM Solution, undertaking as per Annexure- XX on their company's letter head should be provided. Provide CA Certificate as per Annexure- XIII and Audited Financial statements (Balance sheet and Profit & Loss statement) for three (3) financial years. The CA certificate provided in this regard should be without any riders or qualification.</p> <p>If the bidder is already working in a Scheduled Public/Private sector Bank in India and is a wholly owned subsidiary of a global OEM/OSDs operating in India, the global turnover may be considered for the last 3 financial years viz. 2026, 2025 and 2024 subject to an unconditional undertaking from the Parent Company for completion of the proposed project, in case the bidder (wholly owned Indian subsidiary) defaults or fails to honour the RFP/Contract.</p>
4	<p>The bidder should be profitable organization on the basis of profit after tax (PAT) for at least 02 out of last 03 financial years mentioned in para 3 above.</p> <p>The net worth of the Bidder should not be negative on 31.03.2026 and also net worth should have not eroded by more than 30% (thirty per cent) in the last three years ending on 31.03.2026.</p>	<p>Self-attested Copies of audited financial statements duly certified by auditor along with the auditor's report to be enclosed. Along with the net worth certificate for last three years ending 31.03.2026.</p> <p>If the bidder is already working in a Scheduled Public/Private sector Bank in India and is a wholly owned subsidiary of a global OEM/OSDs operating in India, the global net worth may be considered for the last 3 financial years viz. 2026, 2025 and 2024 subject to an unconditional undertaking from the Parent Company for</p>

S.No.	Criterion	Documentation Required
		completion of the proposed project, in case the bidder (wholly owned Indian subsidiary) defaults or fails to honour the RFP/Contract.
5	Bidder and OEM not debarred/blacklisted by Govt. of India / State Governments / Regulatory Agencies / PSUs / other institutions at the time of submission of bid and Bidder not insolvent, bankrupt, in receivership, or being wound up.	Self-Declaration (Annexure — II).
6	Bidder/OEM/OSD in EFRM software business for minimum 5 years as of bid date. In case of the OEM/Bidder is MSME the experience required is 3 years as on 31.03.2026.	PO copies and Go-live / satisfaction letters from clients.
7	Proposed solution / transaction monitoring system live at minimum 2 Scheduled Commercial Banks/RRB in India. One \geq 1,500 branches; one \geq 1,000 branches. Live \geq 2 years as of 31.03.2026.	Self-declaration / OEM / OSD letter with name of banks and supporting document issued by other banks / PO copy can be provided in support along with Annexure-XII.
8	Bidder/OEM should have integrated experience in EFRM solution / transaction monitoring system with minimum 3 channels out of following mentioned channels in single implementation: <ul style="list-style-type: none"> 7. CBS 8. Internet Banking 9. Mobile Banking 10. Debit card 11. UPI (mandatory) 12. AEPS Note: The above clauses are for eligibility purpose only. Bank requires an implementation in real time preventive mode and integration at an enterprise level mandatorily for all the above mentioned channels as well as other channels mentioned elsewhere in the RFP.	Self-declaration / OEM / OSD letter with name of banks and supporting document issued by other banks / PO copy can be provided in support along with Annexure-XII.
9	OEM has development & support centre in India with \geq 150 technical resources on payroll.	OEM certificate on letterhead mentioning centre addresses and headcount.
10	Bidder (who is an authorized representative of OEM) has development & support centre in India with \geq 100 technical resources on payroll (including Architecture, Development, Testing, Business Analysis roles).	Undertaking on Bidder letterhead with addresses and headcount.
11	Certification requirements: The Bidder should possess any three (3) of the below certifications which are valid at the time of bidding: <ul style="list-style-type: none"> 6. Valid ISO 9001:2008/ISO 9001:2015 for quality management system 7. ISO 20000:2011/ISO 20000-1:2018 for IT service management 8. ISO 27001:2013 for Information Security Management system 9. CMMi Level 3 or above for capability Maturity Model Integration 10. PCI – DSS-4.0 	Copy of valid certificate.

S.No.	Criterion	Documentation Required
12	Bidder should have all necessary licences, GST registration, PAN, and statutory approvals as required under the law for carrying out its business. It should have valid GST and other applicable taxes registration certificates/PAN etc.	Undertaking + registration copies.
13	Bidder must provide information that any of its subsidiary or associate or holding company or companies having common director/s or companies in the same group of Promoters/ management or partnership firms/LLPs having common partners have not participated in the bid process.	Self-undertaking on company letterhead.
14	Labour Law compliance.	CA/Statutory Auditor certificate or self-undertaking.
15	Bidder and OEM undertaking that ALL technical and functional features in the Scope of Work are available in the proposed solution.	Undertaking on letterhead (Annexure — XV)

ANNEXURE-XI Pre-Bid Query Format
(to be provided in MS-Excel format)

CARE: Note not to change the format, and also mention the particulars correctly, as per heading. Further, do not merge cells, in rows or columns. Any suggestions of other than general nature, may be incorporated in detail, in the Solution Document.

Bidder's Name:

Vendor	S.No	RFP Page No	RFP Clause No.	Existing Clause	Query details

Signature of Authorized Signatory Name:

Designation:

Date:

ANNEXURE-XII Experience Details/Reference Site Summary

Ref: RFP No.

Dated

(Submit attested photocopies of Purchase Orders as supporting documents for each item as per eligibility & evaluation criteria separately)

S.No.	Name of Organization for whom services rendered	Nature of Work	Channels integrated	No. of branches	Team size	Project Details		
						Period (No. of Months)	Start Date	Date of Completion/expected completion

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

ANNEXURE-XIII Turnover, Net Worth and P&L Certificate

(Bidders have to submit attested photocopies of Audited Balance Sheet / P&L)

Ref: RFP No.

dated

(Amount in Rs.)

F Y	Turnover	Net Profit / Loss	Net worth
2023-24			
2024-25			
2025-26			

Signature of Authorized Signatory

Name:

Designation:

Seal:

Date:

ANNEXURE-XIV BID SECURITY FORM (EMD)/BID SECURITY DECLARATION

(to be submitted at the time of on-line submission of bid)

To,

**General Manager
Fraud Risk Management Department
Uttar Pradesh Gramin Bank
2nd & 3rd floor, NBCC Commercial Complex,
Vardan Khand, Gomti Nagar Extension,
Lucknow - 226010**

Sir,

Sub: Request for Proposal Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

We _____ having our registered office at _____ (herein after called the 'BIDDER') are offering Earnest Money Deposit as per details below for consideration of the bid of the above mentioned Bidder.

Amount : Rs. _____/- (Rupees _____ Only)
Mode : Online Transfer / Bank Guarantee
Payment Type: RTGS (Real Time Gross Settlement) / NEFT (National Electronics Fund Transfer)/ Bank Guarantee

UTR / Txn ref. No.: _____
Txn Date: _____
Remitting Bank _____
Remitting Bank IFSC Code: _____
Beneficiary Account Name : UTTAR PRADESH GRAMIN BANK
Beneficiary Bank Account No. 50010015161020
Beneficiary Bank IFSC Code: BARB0BUPGBX

The details of the transaction viz. scanned copy of the receipt of making transaction or Bank Guarantee or Micro and Small Enterprises (MSE) / Startups Certificate (if EMD not applicable) to be enclosed.

The Bank at its discretion, may reject the bid if the EMD money doesn't reflect in beneficiary account or BG not received as per details furnished above.

Account Details for refund of Bid Security (Earnest Money Deposit) as per terms & conditions mentioned in the Tender document.

We _____ having our registered office at _____ (herein after called the 'BIDDER') are providing our bank account details as per below to be considered as our account for refund of Bid Security (Earnest Money Deposit), wherever applicable as per terms & conditions mentioned in the Tender document.

A/C Name: _____
A/C No. (Company account details): _____
IFSC Code: _____
Bank Name: _____
Bank Address: _____

The details mentioned above is treated as final & bank shall not be held responsible for any wrong/failed transaction due to any discrepancy in above details.

Dated this _____ by _____ 20__

Yours faithfully,

Authorized Signatory

Name:
Designation:
Bidder's Corporate Name:
Address:
Email ID:
Phone Number:

ANNEXURE-XV Functional and Technical Compliance Matrix

Bidders must submit the Technical and Functional Compliance Matrix with responses for ALL items. Scoring: 1 = Feature available Out-of-the-Box; 0 = Feature available through customisation before Go-Live (specify timeline and approach); 0 = Feature not available. Minimum 85% overall score for qualification. Any below item scoring 0 results in automatic disqualification.

Area: General Capabilities

SI No.	Particulars	Yes(Y)	No (N)	Customizable (C)
A.1	Proposed Solution should have ability to failover without/with least manual intervention.			
A.2	Proposed Solution should replicate the data between DC & DR in real time basis or as required by the bank.			
A.3	Proposed Solution should store historical incidents/alerts onsite to correlate future transactions.			
A.4	Proposed Solution should integrate with all existing delivery channels of the Bank as specified in "Scope of Work", point no. 4 above.			
A.5	The proposed solution should take/give feeds from/to various applications of the Bank as specified in "Scope of Work", point no 4 above.			
A.6	For Customer Outreach, the proposed EFRMS Solution should integrate with Bank's various authentication/ gateway solutions as specified in "Scope of Work", point no 4 above.			
A.7	Proposed Solution (System/Application) Should maintain Audit Logs of all user activities including User ID, Date/Time, IP Address etc.			
A.8	Should conform to all regulatory, statutory, legal acts and rules including IT Act, 2000 (Amended 2008).			
A.9	Proposed Solution should have an integrated case management system where the alerts get triggered based on the real-time transaction monitoring performed. Case has to be created within 3 seconds from the time the transaction has been responded by the solution. Cases to be triggered automatically but functionality for manual creation of cases should also be there.			
A.10	Proposed Solution should enable real-time case creation for any fraud/non-compliance patterns identified by the real-time transaction monitoring engine.			
A.11	Proposed Solution should have the ability to manage multiple queues/projects for managing case of certain types e.g staff fraud, 3rd party fraud, staff compliance, KYC compliance, Branch non-compliance etc.			
A.12	Real-time cases should get triggered in the right type of project/queue as per the categorization.			
A.13	Proposed Solution should have access controls available to establish groups of authorized Bank users with different privilege levels.			

A.14	Proposed Solution should have the ability to manage multiple groups of users and assign specific group to specific project/queue including administrator users and parameter users			
A.15	Proposed Solution should have provision for configuration of workflow for alerts/cases as per bank's operational process requirements			
A.16	Proposed Solution should have ability to route and assign cases to the right set of investigators based on pre-defined case routing Logic.			
A.17	Proposed Solution should have ability to define roles and user groups and assign privileges.			
A.18	Proposed Solution should provide complete evidence and list of transactions that cause a scenario match and alert.			
A.19	Proposed Solution should have ability to define and categorize the different types of frauds/non-compliance.			
A.20	Proposed Solution should have Auto and manual linking of alerts to parent entity case.			
A.21	Proposed Solution should configure for Alerts to be sent to appropriate users via SMS or email.			
A.22	Proposed Solution should have ability to manually assign alerts to users.			
A.23	Proposed Solution should have Built in escalation matrix to assign alerts automatically to stake holders for review and assessment.			
A.24	Proposed Solution should have facility for auto-update (list of reasons) of user comments while closing alerts.			
A.25	Proposed Solution should have ability to attach a doc, image, data from other systems to an alert/case in case manager.			
A.26	Proposed Solution should have ability to export the case reports.			
A.27	Proposed Solution should have ability to flag an alert based on the pre-defined criteria (e.g. false positives, suspicion, type of fraud).			
A.28	Proposed Solution should have ability to mark an entity (customer, account, device, IP etc.) to a watch list.			
A.29	Proposed Solution should have ability to send feed back to the fraud prevention engine to reduce false positives and increase fraud prevention rate.			
A.30	Proposed Solution should be capable of generating Real time alerts using artificial intelligence/ machine learning.			
A.31	Proposed Solution should Support complete audit trail for each user action throughout the case life cycle.			
A.32	Proposed Solution should have ability to dynamically calculate risk score associated with the alert based on the triggered patterns, push up criteria & push down criteria (criteria that increases or decreases the risk score)			

A.33	Proposed Solution should have ability to view all alerts corresponding to a particular customer/account under a single parent case.			
A.34	Proposed Solution should have ability to resolve alert into one of the final states e.g. confirmed fraud, false positive etc.			
A.35	Proposed Solution should have ability to categorize the confirmed fraudulent case into one of the categories as per RBI fraud reporting categorization			
A.36	Proposed solution should allow users to manually move or select transactions using a drag-and-drop interface for marking / tagging a suspicious transaction in case manager.			
A.37	Proposed solution should generate alerts based on customer risk category and threshold limit.			
A.38	It should provide facility for prioritization of alerts based on scenarios requirement.			
A.39	Proposed Solution should work on dynamic learning and static rule-based transactions (risk based engine). The system should work on the dynamic profiling of the customer in real time for monitoring current and future transactions of the customers.			
A.40	Solution should support use of standard logical operators (eg: AND, OR, NOT etc) in all Real time Authorization of Rule conditions.			
A.41	Solution should support use standard arithmetic operators (e.g.: >, <=, = etc) in all Real time Authorization Rule conditions.			
A.42	Rules engine should be able to create / modify exclusion criteria, within a rule, to route activity to an exclusion queue.			
A.43	Rules engine should enable the users to interact with recent data to identify the transaction patterns during the day.			
A.44	System should support provision to block a channel facility (for eg Mobile Banking/Internet Banking/UPI/ECOM/POS etc) with respect to any entity.			
A.45	System should support to single click blocking of all the transaction channels.			
A.46	The proposed solution should have the capability to generate Risk score based on both transaction (channel wise) and at customer profile level.			
A.47	The solution should have the ability for each transaction to be evaluated by every rule.			
A.48	The solution should be able to identify the rules triggered by a transaction.			
A.49	The solution should be able to assign weightages /priority to the rules.			
A.50	Support uploads of XML and other files/messages such as XBRL/txt/ASCII/CSV/xls/other standard and proprietary formats including formats from Clearing and Settlement and Dispute Management System.			
A.51	The proposed solution should have the capability to create the rules based on user defined and derived			

	variables using the transaction data.			
A.52	Solution should be able to handle the ISO 8583/ISO 20022/Existing XML Messages.			
A.53	Solution should be able to handle the Reversal messages in both ISO and XML format sent by the respective switches.			
A.54	Rules engine should enable the users to simulate the various levels of thresholds for the variables identified to indicate the number of alerts that will get generated.			
A.55	The solution should have the ability to compress the data.			
A.56	The proposed solution should have the capabilities to integrate Open & Enterprise APIs with Banks middleware solution.			
A.57	The solution must be able to use the inputs from the online fraud monitoring services (anti-Phishing, anti-Pharming, anti- Trojans, anti-Rogue etc) such as suspected IPs, suspected locations, compromised accounts, Mule account details used by various Trojan families, dummy data fed to fraud sites etc and other inputs provided by the bank and third parties.			
A.58	Solution should be bundled with a General rule library which should include rules that are suitable to counter present and evolving fraud trend scenarios ,the rule library should be customisable as per the requirement of Bank.			
A.59	Solution should have ability to define clusters using several different techniques and relations.			
A.60	The user access management at application level should be able to restrict the rights to delete/modify/recreate workflow steps of certain users.			
A.61	The proposed solution should automatically trigger alerts through Mail/SMS to concerned stake holders if there is no Heartbeat or Response from the EFRMS.			
A.62	Solution should support ability to execute rules in test mode against production data and analyse the impact of such a rule based on the output of the alert.			
A.63	The Solution should support detailed Threshold Analysis, in order to fine tune alerts and reduce false positives.			
A.64	The solution should provide analytical capabilities for: Correlations & Regression, Network plot Decision and Tree Scenario analysis.			
A.65	The proposed solution should provide complete evidence for why a transaction was declined/hold by the fraud management system.			
A.66	The proposed solution should support built-in maker-checker functionality to ensure dual commit to critical system changes.			
A.67	The solution should support risk score model (or equivalent) where many minor cues can add up to a risk score which in turn can trigger an action.			

A.68	The solution should support & leverage the knowledge of already identified historical frauds when authoring new rules.			
A.69	The proposed solution should have the ability for additional review(s) of case disposition based on several factors (role, tier, delegated authority, etc.)			
A.70	The solution should allow data to be accessed from any industry standard data source using native connectors and load the same in Memory.			
A.71	Solution should have the ability to consume data in the source format without any dependency from the individual switches.			
A.72	The various source channels may share Account number/Card Number/ Masked Aadhar number/Mobile number/CIF etc in the financial/non-financial messages. The proposed EFRM Solution must carry out the monitoring across all transaction channels strictly based on Customer Identification Number (CIF no) only.			
A.73	The proposed solution should not have any limitation as to no. of rules/scenarios/policies that can be configured for fraud prevention and detection.			

Area: Real time fraud prevention, detection, scoring engine and case manager

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
B.1	Proposed solution should support both real time and near real time transaction processing i.e. after the response has been provided.			
B.2	The integration should not affect the performance of the source systems. Integration required to the Uttar Pradesh Gramin Bank environment has to be done at no extra cost and will be the sole responsibility of the bidder including minor enhancements.			
B.3	Proposed solution should support cross-channel frauds & non-compliance prevention and detection in real-time.			
B.4	Proposed solution should consist of a hybrid fraud prevention model consisting of pre-packaged scenarios, behaviour profiling and predictive scoring models with proven low false positives and high fraud prevention rate as well as user defined scenarios.			
B.5	Proposed solution should support an advanced rule/scenario engine to prevent known fraudulent patterns.			
B.6	Proposed solution should allow end user to easily configure scenarios parameters using a web-based interface and be able to deploy in the production environment.			
B.7	Proposed solution should allow to include wide range of parameters including but not limited to transaction parameters, customer profiles and account attributes, IP			

	and device parameters to be used in scenario building.			
B.8	Proposed solution should be able to dynamically increase or decrease the risk score of a fraudulent pattern based on good and bad customer/account behaviour even after a case is generated to reduce false positives and increase fraud prevention rate.			
B.9	Proposed solution should support machine learning based behaviour profiling and anomaly detection engine that continuously monitors customer/account behaviour and builds positives profiles in real-time.			
B.10	Proposed solution should provide the list of behaviour profiles supported in the system and necessary documentation for the same.			
B.11	Proposed solution should support product/channel specific fraud scoring models.			
B.12	Proposed solution should be able to recognize/identify the transaction characteristics by channels/transaction type/ account number/ CIF/mobile no/ customer profile and enforce the respective policy of the bank on a real time basis and apply specific risk and fraud rules.			
B.13	Proposed solution should be able to correlate transactions across all the integrated channels (For ex. UPI, Debit Card, Credit Card, Omni Channel, AEPS etc.) in a real time basis and prevent cross channel frauds as opposed to silo based approach. Scenarios will be defined as per the Bank's requirement across all integrated channels			
B.14	Proposed solution should be able to auto mark customers/accounts into various groups and watch lists based on case feedback.			
B.15	Proposed solution should be able to detect common point of compromise and mark those entities into blacklist/watch lists.			
B.16	Proposed solution should have an option of adding customers in Blacklist and Whitelist manually/upload. These lists should be applicable across all channels.			
B.17	Proposed solution should support various business policies to approve/decline/challenge/hold/delay transactions based on the hybrid fraud risk score.			
B.18	Proposed solution should automatically adjust the risk score of scenarios based on false positives occurrence (marked).			
B.19	Proposed solution should facilitate categorization of cases based on the risk score of detected fraud pattern.			
B.20	Proposed solution should have ability to send notifications via SMS/Email or out bound call through call centre representatives & IVRS as and when a case is created.			

B.21	Proposed solution should have inbuilt auditing and logging functionality. All events should be logged and be available to support investigation related to fraud incidents and other uses through user friendly GUI in the solution itself.			
B.22	Proposed solution should be able to monitor and detect both financial and non-financial transactions including various branch user exceptions.			
B.23	Proposed solution should be able to provide both real-time transaction monitoring and transaction blocking/hold feature for suspicious transactions.			
B.24	Proposed solution should support import of data from various software/database in different formats like Excel , Text, Delimited Text, XML, CSV, PDF etc. and convert/store them in readable or executable format for further processing.			
B.25	Proposed solution should Support wide range of interface protocols (tcp/ip, web service, http/https etc.) and message formats (JSON, ISO 8583, XML, MQ, ISO20022, fixed width format, SOAP, REST etc.)			
B.26	The proposed solution efficiently handle high transaction volumes with real-time processing, making it suitable for large-scale banking environments to be proven upto minimum 3000 tps and to be scalable upto 10000 tps.			
B.27	Proposed Solution should implement enhanced authentication through various modes i.e. SMS-OTP, Email, PKI Authentication, TOTP, Challenge- Question based on Transaction Scoring generated by the Solution as per Bank's requirement.			
B.28	Proposed Solution should provide Real-Time Dash Board & Alerts for multiple Role Based Users and based on different domains/Channels.			
B.29	The proposed solution should provide advanced case management system that should cover cases generated from all source channels.			
B.30	The case management system should be able to segregate the cases of customer across the channels.			
B.31	Proposed case management system should support configurable work flow based on the case type, and built-in auto case routing mechanism.			
B.32	Proposed case management system should have the ability to create, edit and view a case based on user permissions.			
B.33	Proposed case management system should have the ability to set default fields and values on screens based on case type.			
B.34	Proposed case management system should be configurable with automated IVRS and based on the response from IVRS the case management system should have the capability to publish the alerts with			

	suitable tag for further action and communicate with CBS middleware for blocking the account in case of a fraudulent transaction.			
B.35	The proposed solution should be able to integrate alerts of all channels with IVRS for automatic calling.			
B.36	Proposed case management solution should support case escalation feature based on business policies configured.			
B.37	Proposed case management solution should be configurable with systembased telephone diallers/auto diallers.			
B.38	Proposed case management solution should be able to simultaneously cater to at least 100 to 150 simultaneous login without any performance bottle necks.			
B.39	Proposed case management solution should have the ability to be able to instantly update existing cases with fresh transaction detail.			
B.40	Proposed case management solution should have ability to link cases under investigation, elevate an alert into a case, add several alerts to one case.			
B.41	Proposed case management should have easy search option for searching the cases with any of unique identifiers like Account number, Customer ID ,Mobile ,PAN etc .			
B.42	The proposed case management solution should create an audit record containing the identification of the user, a timestamp, and date when actions are performed to a case that may be provided to management, an examiner, or regulating agency.			
B.43	The Case management solution UI should Mask the Debit/Credit Card details as per PCI-DSS standards.			
B.44	The case Management solution provided should have the capacity to handle alerts of at least 6 months. Post which the bidder should provide a suitable archival strategy.			
B.45	The bidder has to provide the hardware/system software sizing for data archival solution in order to store the complete data being generated during the contract period, Sizing for both DC & DR to be provided by the bidder as specified in the RFP. Bidder has to ensure that a minimum of 9 months' data should be available in the Case managementsolution.			
B.46	There should be no lag in loading of User Interface (UI) of Case Manager Application with relevant transaction data. The required information should be available to the Fraud Analyst in the UI within 3s of the actual transaction and should not be affected by the number of alerts present in the system.			
B.47	In case of reopening of past transactions or cases where Bank requires the alert data which has already been archived, the bidder has to provide a suitable			

	data retrieval strategy.			
B.48	Rule engine should have the ability to delete or remove workflows if they become redundant.			
B.49	Solution should support dashboard for rule administration to identify the rules that need optimization.			
B.50	Solution should have ability to alert when the false positive rate or the detection rate breaches a particular threshold.			
B.51	Case management solution should display all the related details like customer information, profiles, rules violated, past investigated transactions to be available to the analyst when he/she attends a case associated with an alert.			
B.52	Reminder generation facility must be available when the case is about to breach the time frame allowed or expiry date time is getting closer.			
B.53	All the cases assigned to the analyst must be viewable in a single window in tabular form. The user should be allowed to hide/unhide attributes/columns of the cases selectively.			

Area : Core Banking Solution

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
C.1	Vendor should be capable of integrating the proposed solution with Bank's CBS and other related systems.			
C.2	Proposed solution should be able to correlate core banking transactions with other direct channel transaction for cross- channel fraud and compliance management in real-time.			
C.3	Proposed solution should be able to monitor user/branch/region level exceptions real-time and provide real-time alerts when the defined thresholds are breached.			
C.4	Proposed solution should provide pre-packaged scenarios to detect various external and internal frauds and non- compliance issues including suspicious inquiries, account take over, nepotism, surveillance avoidance, exceptions, misuse of authority, sudden surge in transactions, unusual behaviour, compliance and improved fraud analyst understanding.			
C.5	Proposed solution should have the flexibility to define/configure new fraud scenarios using a web based tool without the need for any code changes. This tool should enable building of new real-time fraud scenarios based on the core banking transactions and master data attributes.			
C.6	Scanning through transactions based on multiple attributes and provide breaches to the threshold of the			

	transactions as alerts/denials/challenges in real time and also as lists/reports.			
C.7	The bidder should ensure that the proposed solution does not impact the performance of any of the bank's systems and databases including the Core Banking System (CBS).			
C.8	Solution should consist of a hybrid fraud detection model consisting of configurable scenarios, behaviour profiling of customers for example based on profession such as student, Housewife, salaried, businessman, professionals, trust, society etc. or any other criteria with proven low false positives and high fraud detection rate.			
C.9	Proposed solution should monitor specific general ledger account and identify suspicious debit/ credits in general ledger accounts based on the real time transaction monitoring.			
C.10	Proposed solution should be able to detect suspicious frauds & non-compliance patterns at both individual user/employee level and overall branch level.			
C.11	Proposed solution should have the capability to identify suspicious transactions attempted on dormant, near-dormant and deceased accounts based on the real-time transaction monitoring.			
C.12	Proposed solution should have the capability to perform specific transaction monitoring and fraud detection/non-compliance scenarios for new accounts (say accounts of vintage less than 6 months).			
C.13	The proposed solution should monitor Internal Accounts, Deposit accounts, Loan accounts, Staff Accounts, New Accounts, Money mules, CTS, NACH, PFMS, Account Disbursement services etc.			
C.14	The proposed solution should have the capability to handle the Bulk approval Payment events.			
C.15	Proposed solution should have the capability to identify suspicious employee activities (balance enquiries, exceptions, EOD, TODs, charge waivers etc.) based on the real-time transaction monitoring.			
C.16	EFRMS should have the ability to detect fraudulent account opening and closure events (e.g. Rapid account opening with high value transactions and immediate closing) done using employee details.			
C.17	EFRMS should have the ability to detect potential fraudulent accounts opened in the name of employees and indicating suspicious transactions.			
C.18	The proposed solution should monitor Employee or related accounts with high credit limits receiving high number of transactions.			
C.19	The proposed solution should monitor Accounts with high balances that are closed by an employee.			
C.20	The proposed solution should handle the Batch transactions from CBS & Exim channels where there may be a (i)single debit and a single credit, (ii)single			

	debit and multiple credits, (iii)multiple debits and a single credit or (iv)multiple debits and multiple credits in a single batch.			
--	-------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Area: Non-financial Transactions from all Channels

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
D.1	Solution should monitor Non-financial transactions that include frequent PIN/ Password change in Cards/Internet Banking/Mobile Banking etc.			
D.2	Solution should monitor any additions, modifications, deletions to vital fields in Account, Customer Master files maintained in CBS system.			
D.3	Solution should monitor for events like frequent password resetting of the teller in Core Banking System.			
D.4	Solution should monitor for Customer Risk Profile changes from Higher to Lower classification.			
D.5	Solution should monitor Frequent locker operations (entries made in CBS).			
D.6	Solution should monitor for sanction of multiple or high number of small loans on a particular given day disproportionate to average sanction made by the said branch.			
D.7	Solution should be able to segregate customers who are having Common mobile number, Email ID, PAN, landline number, communication address, Aadhaar card number in multiple customer IDs.			
D.8	Solution should monitor for Issue of large number of cheque books in an account within a short time frame.			

Area: Mobile Banking/Internet Banking

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
E.1	Proposed solution should have the capability to detect anomalous customer behaviour or transactions originating from Omni channel.			
E.2	Proposed solution should use the risk-based scoring model that is used to establish normal customer behaviour and determine anomalous behaviour. The model should learn over time by itself.			
E.3	Proposed solution should analyse Multiple data to contribute to the model assessment score and risk score this should include: - Transactional Information, i.e. Device info, session data, Account ID etc. - Data Enrichment information, i.e. IP geo location, ISP, connection type, IMEI Number, other unique device information etc. - Profiling Data, i.e. Account ID, IP address, Device fingerprint, Payee ID, Account activity after login etc.			

E.4	Composition of risk score should be transparent to Bank (i.e. the exact reason for a high score will be available to Bank staff to enable accurate decision-making).			
E.5	Proposed solution should have the ability to monitor all pre-login, login and post login transactions to detect any suspicious patterns.			
E.6	Proposed solution should provide pre-packaged scenarios to monitor pre-login, login and post login fraudulent patterns.			
E.7	Proposed solution should be able to detect & prevent following fraud schemes including but not limited to: - Identity theft and account take over as result of phishing attack, malware attack and social engineering attacks, Man-in-the-browser, Man-in-the-middle attacks, Transaction Velocity Check, Suspicious Beneficiary registrations and unusual funds transfer, Sudden Transaction Amount Surge compared to established customer/account profile, Sudden Transaction Volume Surge compared to established customer/account profile, Personal Details Change (Mobile Change, PIN change etc.), Transaction from non-predominant IP, ISP, IP Country, IP City, device, odd hours compared to established profile, Entity white list and black list for IP, ISP, IP Country, IP City, device id, e-banking user id, mule account etc.			
E.8	Proposed Solution should support advanced IP geo-intelligence capabilities to deduce IP Country, IP City, Proxy IP, ISP etc. from the transaction IP address. These facts should be available in the GUI for framing policies.			
E.9	Proposed Solution should have capability to build and re-factor dynamic e-banking user behaviour profiles including but not limited to: -Preferred Country - Preferred City - Preferred IP -Preferred ISP -Preferred Device -Preferred Payee -Average Daily/Weekly/Monthly Funds Transfer amount by payee/biller -Average Daily/Weekly/Monthly Funds Transfer volume by payee/biller -Preferred Transaction hour.			
E.10	Proposed Solution should provide well defined API for integration with host internet banking and mobile banking system for real-time decision making supporting wide range of interface protocols and message formats.			
E.11	Proposed Solution should have the capability to take external lists data as input to detect any known fraudsters/compromised devices/IPs etc. The external list data could be the data shared by regulators, IBA, NPCI, CERT-IN etc.			
E.12	Proposed Solution should be able to consume externally sourced entity for example Neustar, Maxmind, Lexis Nexis, Group-IB, RSA information			

	(e.g. IP addresses, destination accounts etc.) etc. to identify known fraudulent activity. The system should also have the facility to export the entity data corresponding to confirmed fraud cases within the bank so that the data can be shared with external agencies like the Regulators, IBA etc.			
E.13	Proposed system should support setting limits on the number of Internet Banking beneficiaries that may be added in a day per account and provide alerts based on a threshold number of beneficiaries.			
E.14	Proposed system should put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.			
E.15	Proposed system should ensure additional factor of authentication/ step up authentication for payment/login/non-financial events based on the policies.			
E.16	Proposed solution should be able to monitor the Fund transfers within own accounts, transfer to other accounts within the Bank.			
E.17	Proposed solution should be able to monitor the Standing Instruction set and Recurring transactions happening in Mobile and Internet Banking (Omni Channel).			
E.18	Proposed solution should be able to monitor the Fund transfers to other Bank accounts through Various modes like NEFT, RTGS, IMPS etc.			
E.19	Proposed solution should be able to monitor the Shopping/Bill Payment/Lifestyle events initiated from Omni Channel.			
E.20	Proposed solution should be able to configure policies based on non-financial events like Add Payee, Frequent Logins etc.			
E.21	Proposed solution offered should utilize device identification or machine fingerprinting.			
E.22	Solution should be able to ingest the risk score received from Channels like Adaptive authentication , Behavioural Biometric solution and update the profile of the customer based on the same.			
E.23	EFRMS should have the ability to generate alerts in dormant accounts where there are unusual large transactions made through mobile application.			
E.24	Proposed solution should have the capability to support all types of browser and operating systems environment on all devices e. g Personal Computers/ Laptops/Smart phones/ TABS/ other devices.			

Area: AI/ML

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
F.1	The AI and ML capabilities of the solution including the kind of model (Supervised or Unsupervised) should be clearly documented and demonstrated by the selected bidder.			
F.2	The proposed solution should have the capability to integrate with AI/ML solutions that may be provided by the Bank in addition to the inbuilt AI/ML capabilities.			
F.3	Demonstration of ML models' ability to adapt and learn from new fraud patterns and data in real-time to continuously improve accuracy.			
F.4	Demonstration of vendor's solution for real-time fraud scoring that assigns a risk score to each transaction based on historical data and AI models.			
F.5	Details on the vendor's XAI (Explainable AI) capabilities to ensure transparency in model decision-making for regulatory compliance and improved fraud analyst understanding.			
F.6	Vendor should be able to demonstrate tools and techniques for data preparation, feature engineering, and handling imbalanced datasets common in fraud data.			
F.7	Solution should use financial & non-financial transactions for behaviour profiling (scoring model).			
F.8	Solution should have ability to include different sets of limits and thresholds for different event types.			
F.9	Solution should provide bank with the capability to create, modify & delete models without any vendor dependency through GUI.			
F.10	There should be no restriction on the number of Models which can be deployed by the Bank.			
F.11	Solution should provide the capability to define, create, modify the parameters used for risk score and the parameters that can be used for cross channel analysis.			
F.12	The solution should be able to compare between 2 or more existing models with the new model to understand the efficacy of the models.			
F.13	The solution to have a Self-Learning Risk Engine.			
F.14	The solution should be integrated with Analytical Models for fraud risk for last 3 years or versions. Model performance report for last 3 years or versions to be submitted.			
F.15	Machine Learning proposed should be available at both macro level as well as hyper personalized level. ML models should continuously evolve			

Area: Customer Profiling & MIS

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
G.1	Solution should have the capabilities to create comprehensive individual customer profiles based on various parameters like Demographics of customer , Digital Channels availed, Annual Income declared etc.			
G.2	Solution should update profiles in real time with every new transaction or event on the entity.			
G.3	The solution should have the capability to enrich data received from various data sources so that they can be used to profile the customer.			
G.4	Solution should be able to create scores that are portfolio specific and/ or relationship specific based on the profiles created.			
G.5	The solution should have the capability to identifying linkages between different entities based on the transactional relationships based on the customer profiles and dynamically adjust score in cases which are suspicious.			
G.6	Solution should be able to run link analysis between multiple CIFs, accounts, customers, transactions for commonality in the various possible parameters like common mobile number, common beneficiary, common address, common modus operandi etc.,			
G.7	The proposed solution should provide information to demonstrate account linkages, transaction movement across various entities. Solution should be capable to capture relationships based on transactions, accounts, customer profile, customer demographics etc., it should have capability to provide transaction pattern analysis.			
G.8	The proposed solution should support building of scenarios across various banking channels like IMPS, UPI, Omni, RTGS, Debit Card, Credit Card, AEPS etc and there should be no restrictions in the no/type of channels used for framing policies. The proposed EFRM Solution must carry out the monitoring across all transaction channels strictly based on Customer Identification Number (CIF no) only.			
G.9	Proposed solution should provide built in pre-packaged report and dashboards to monitor no of open, in progress and closed cases, false positive trend, fraud detection rate and savings, investigators' performance.			
G.10	Proposed Solution should allow business users to create their own dashboard and reports using a drag and drop graphical interface.			
G.11	Proposed Solution should allow end users to create custom reports using wide range of attributes including transaction attributes, case attributes, customer and account attributes.			
G.12	Proposed Solution should support wide range of dashboard widgets to create different types of dashboards including pie chart, bar chart, bubble			

	chart, heat maps, angular chart etc.			
G.13	Proposed Solution should allow to export dashboard and reports to various formats including pdf, xls, html, Power BI etc.			
G.14	Proposed Solution should allow to configure these reports and dashboards to be sent to list of users via email.			
G.15	Proposed solution should allow complete slicing and dicing of reports and dashboards across various dimensions like product, channel, geography etc.			
G.16	The solution should support defining the rules at multiple levels like transaction, CIF, account, customer/group of customers and also any additional information from unstructured stored in a separate database within EFRMS or from external systems.			
G.17	Solution should visually prepare data for analysis, including joining tables, defining custom calculated columns and creating custom expressions for data tables available.			
G.18	The proposed solution should provide pre-packaged MIS dashboard and reports for tracking fraud cases, investigators' performance and system performance. and system performance and ensure Reports / rule simulations, concurrent usage by various users of entities should not have any impact on performance.			
G.19	The Solution should be able to generate periodic (Daily, Weekly, monthly etc.) customized reports to the Bank as per Bank's requirement.			
G.20	Solution should be able to Capture and report impact, loss averted, benefits realized.			
G.21	Solution should be able to provide summary Report which provides insight into the work that is being done by fraud investigators and the effectiveness of the fraud analysts at resolving alerts to be made available to admin users.			
G.22	Solution should provide a summary report which summarizes the newly scheduled alert information to be made available to admin users.			

Area: Channel Specific & Mule detection

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
--------	-------------	--------	-------	------------------

H.1	Proposed Solution should support out of the box behaviour profiles including but not limited to Card holder profiles, Preferred ATM machines, Preferred Merchants, Preferred Merchant Category Codes, preferred Country /City ,Preferred Time Period, Preferred Transaction hour for ATM, POS, E-Commerce, Preferred Currency for purchase-Average Daily/ Weekly/ Monthly/ Quarterly / Season based transaction amount by channel (for domestic and international transactions), Average daily/Weekly/Monthly/Quarterly/Season based transaction frequency by channel (for domestic and international transactions).			
H.2	Proposed Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.			
H.3	The proposed solution should be able to directly integrate with switch to monitor Debit card transactions across ATM, POS and E-Commerce channels on real time. The proposed solution should support payment card fraud prevention against skimming, counterfeit cards, lost and stolen cards, Mass card compromise, sudden surge and anomalous behaviour, zone hopping in real time Dynamic enablement/ Disablement.			
H.4	The proposed solution should be able to combat both card present and card not present frauds in real-time.			
H.5	The solution should have capability to develop scenario and models related card transactions as per the need.			
H.6	Proposed Solution should support to set threshold limit with specified time periods for all cards that have not been used for international transactions in the past.			
H.7	Proposed Solution should support to set threshold limit with specified time periods for all cards which may be used by few customers internationally, on request.			
H.8	Proposed Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.			
H.9	Proposed system should look for anomalous Card activity, It should detect behaviour associated with a fraudulent transaction.			
H.10	Solution should handle ISO 8583 based Advice message ((0120/220/420 message from Switch (ATM & AEPS)).			
H.11	Solution should handle ISO 8583 based Financial (0200)/400 / Authorization (0100) message from Switch (ATM & AEPS).			
H.12	Solution Should be able to detect the Nonfinancial transactions made through ATM which includes Balance enquiry ,Mini statement ,PIN change etc.			

H.13	Solution should be able to detect the POS Pre-auth, POS refund transactions.			
H.14	The solution should cover other behavioural aspects than per user, e.g. per account behaviour, per beneficiary/receiver behaviour, per IP-address behaviour, per device-id behaviour for UPI.			
H.15	The solution should detect online banking sessions conducted from out-of-footprint geographies.			
H.16	The solution should identify transactions that are originated from high-risk internet service providers Domains, and flag sessions conducted from multiple locations in a short period of time.			
H.17	The Solution should alert on high velocity of pay-outs to multiple accounts through digital channels in short period of time in same day.			
H.18	The proposed solution should have the capability to detect login, pre-login and post login frauds for UPI. It should support advanced IP Geo location tagging capability to detect IP country, IP City, Proxy IP and zone hopping.			
H.19	Solution should monitor Average Daily/Weekly/Monthly Funds Transfer amount / frequency by payee / biller and also preferred transaction hours for all channels.			
H.20	Bidder should be able to integrate with any of risk-based authentication solution (Step UP) for internet banking, mobile banking, e-commerce payments, UPI that will be provided by the Bank.			
H.21	Solution should support various UPI transactions (P2P,P2M,M2P etc).			
H.22	Solution should be able to handle the financial and non-financial XML messages received in case of UPI & IMPS.			
H.23	Solution should be able to ingest the risk score received from Channels like Adaptive authentication , Behavioural Biometric solution and update the profile of the customer based on the same.			
H.24	Solution should be able to detect the new UPI registrations and provide the feedback to the system based on the customer profile.			
H.25	Solution should be able to accommodate rules based on the Location Information derived from AePS transactions.			
H.26	Solution should be able to determine money mule accounts based on various parameters like Geolocation, Turnover in the account, transaction velocity, odd hour, balance enquiry etc.			
H.27	Solution should dynamically enhance the monitoring for suspected money mule accounts based on the Red flags in the accounts (Login to Mobile banking/Internet banking app frequently ,constant change in area of customer ,sudden surge in ecom/ATM, IMPS, UPI transactions) etc.			

H.28	Solution should increase the risk score of the potential money mules and separate queue for these to be created in case management application.			
H.29	Solution should have enhanced due diligence for customer profiles based on the age of account and the number of transactions performed across the digital channels.			
H.30	Solution should dynamically adjust the risk score based on the age ,type of accounts ,Demographics and the amount of credits being received to the account.			
H.31	Solution should detect money mule accounts based on deviations from normal behaviour by using the statistical and machine learning techniques.			

Area: Technical Specifications

SI No.	Particulars	Yes(Y)	No(N)	Customizable (C)
I.1	Solution should be able to integrate to load data into an Operational Data Store and Data Lake as per the requirement of the Bank.			
I.2	Application should handle automatic switchover in cluster environment.			
I.3	Proposed Solution should have ability to failover without manual intervention.			
I.4	Proposed Solution Should be able to support different protocols (TCP/IP, IPX etc.). It should support IPV6.			
I.5	Proposed Solution should implement application patches and updates as specified in "Upgrades & Updates", sub-section 6 above.			
I.6	Proposed Solution should support all the requirements mentioned in "Scope of Work" & "Other Requirements" specified in sub-section 3 & 4 above.			
I.7	System should track the client's IP, Network interface address and device.			
I.8	The solution should have the capability to support archiving the data on HDD/ Peripherals and retrieve from the above for the purpose of processing.			
I.9	Support for integration with packages like chart generators, Statistical/ Financial DLLs, MS Office Components, Power BI etc.			
I.10	Database link, Data, Dictionary and support should be provided to Bank's Data Warehousing & MIS project to enable them to generate the reports in Bank's formats without any additional cost.			
I.11	Selected bidder should ensure that the solution is hardened as per the Secure Configuration provided by the Bank.			
I.12	Proposed solution should be able to cater to cloud data storage.			
I.13	Proposed solution should be compatible with Bank's IPv4, IPv6 and TLS versions.			

I.14	The system should enable profiling of users and definition of control levels and passwords.			
I.15	All Error messages must be logged. It should be possible to look up online (by error message number or by alphabetical list) all error messages reported by the system, to determine their meaning and the appropriate corrective course of action. Error messages or events of a certain severity level should be immediately notified to the System Administrator's Group and actual user.			
I.16	System should provide auditable management of User-ids, access rights and passwords, login, activities etc.			
I.17	Maintenance of a secure, auditable log of access to the system, identifying user- Id, date, time, functions accessed, operations performed etc.			
I.18	Ensure data confidentiality and integrity at rest as well as in transit.			
I.19	Solution should support encryption as per industry standard encryption algorithms			
I.20	A Separate Login/Role / user type is required for Auditors who can view all the parameters / test cases / pending reports/ and perform complete Audit / reporting through the user. Though the audit user would have view permission only.			
I.21	Daily activities log must be merged into the history log files.			
I.22	Enterprise Data Dictionary documents of the solution should be available.			
I.23	Service Lifecycle Management documents should be available.			
I.24	Date, time and User stamped process list for different processes.			
I.25	Provision for daily activity report/s to highlight all the processes invoked.			
I.26	Provision for recording of all unsuccessful login attempts.			
I.27	The solution should be Platform Agnostic and not be constrained to a single Hardware Platform/Operating System/Database etc.			
I.28	The bidder to design the solution, security, and data flow architecture in-line with the Bank's environment			
I.29	The bidder to develop, configure, customize, and implement the solution according to the project scope, technical specifications and functional specifications within the timelines			
I.30	The bidder to ensure solution scalability and performance in line with Bank's business projections and expected performance levels (SLAs)			
I.31	Testing of the proposed solution to also include Unit Testing, System Integration Testing, Performance Testing and Load Testing.			
I.32	Successful Bidder to fully support the UAT, security review, audits, or any other testing requirements of the Bank during the entire contract period			

I.33	Bidder to fix any vulnerabilities/bugs/issues in the platform at no additional cost			
I.34	Must the have capability to support Security mechanism such as TLS v1.3 and above, AD- Integration, Certificates and Key			
I.35	Secure exchange of payment messages not limited to secure message queues, secure file transfer, secure API.			
I.36	Data Replication should be hash encrypted at storage over the network at least SHA1+Salt			
I.37	The Solution should ensure Data Integrity using internationally accepted hashing algorithms such as MD5/ SHA-2 or higher etc. and support standard algorithms like AES.			
I.38	The Solution should support Anonymization (Removing PII), Pseudonymization (Replacing PII with artificial Identifiers) also Data minimization technique to be followed.			

Note:

1. All of the above points are mandatory. Bidder must comply with each of these mandatory line items. Non-compliance to any one or more rows item under those heads will disqualify the bidder.
2. Each line item under Functional & Technical specification will be given a score of 1, if it is already available in the product.
3. Each line item under Functional & Technical specification will be given a score of 0 if it is not already available in the product but is customizable before Go Live of the proposed solution.
4. However, if any point in the Functional or Technical Specification is neither available in the product nor is customizable, the bidder will be disqualified.
5. The total marks allotted to the bidder for the 284 Technical & Functional points will be rationalized to a total of 35 and will be taken to Technical Evaluation Stage 2-Technical evaluation Matrix in section 12.

ANNEXURE-XVI Commercial Bid Format (Table A,B,C,D – Bank-wise)

Applicable only for Technical and Functional
(not applicable for any other terms and conditions stipulated in this RFP)

We / M/s..... confirm that the below-mentioned table has all the 'Customisable sections of Functional & Technical Specifications, of this RFP. Any requirement not covered under this format would be considered as compliant.

We also confirm that all the partially complied or not complied with requirements in sections of Functional Specifications, Technical Specifications will be complied with before Project Go live.

We also undertake to comply with the guidelines in respect of timelines stated in this RFP, failing which we shall be liable for the penalties and other costs recoverable by the Bank.

Sr. No.	Document	Section	Subsection	Line / Sr. no	Requirement	Deviation if any	

Authorized Signatory

Name: Designation:
Bidders' Corporate Name:
Address:
Email and Phone:

ANNEXURE-XVII Labour Law Compliance Certificate

To,

Date

The General Manager
Fraud Risk Management
Department, 2nd Floor, Uttar
Pradesh Gramin Bank Head Office
NBCC Building, Vardan Khand Gomti
Nagar Ext ext, Lucknow-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

We confirm that the employees engaged by our Company to carry out the services in your bank for the above said contract are paid minimum wages / salaries as stipulated in the Government (Central / State) Minimum Wages / Salaries act in force. All the employees/operator deployed by the vendor for the digitization activity must comply with government's rules and regulations like minimum wages act, Provident Fund and ESIC facility standard. We also indemnify the Bank against any action / losses / damages that arise due to action initiated by Commissioner of Labour for non-compliance to the above criteria.

We further authorize the Bank to deduct from the amount payable to the Company under the contract or any other contract of the Company with the Bank if a penalty is imposed by Labour Commissioner towards non-compliance to the "Minimum Wages / Salary stipulated by government in the Act by your company.

Authorized Signatory

Name:

Designation:

Bidders' Corporate Name:

Address:

Email and Phone:

ANNEXURE-XVIII Authorization Letter (Power of Attorney)

SUB: RFP for Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

We have carefully gone through the contents of the above referred RFP and furnish the following information relating to Technical Bid/Specification.

No.	Particulars	Details to be furnished by the Bidder
a)	Name of the Bidder	
b)	E-mail address of contact person(s)	
c)	Details of: Description of business and business background Service profile & Client profile	
d)	Details of similar assignments executed by the OEM/OSD/Bidder during the last five years in India (Name of the Bank, time taken for execution of the assignments and documentary proof from the Bank are to be furnished)	

Authorized Signatory

Name: Designation:

Bidders' Corporate Name: Address:

Email and Phone

ANNEXURE-XIX Manufacturers' Authorization Form (MAF)

No.

Date:

To
The General Manager,
Fraud Risk Management
Department, 2nd Floor, Uttar Pradesh
Gramin Bank
Head Office NBCC Building, Vardan Khand
Gomti Nagar Ext ext, Lucknow-226010

Sub- MAF for your RFP No. **dated**

Dear Sir,

We who are established and reputable manufacturers / developer of (Name of product offered) do hereby authorize M/s..... (Name and address of Agent) to submit a Quote, and sign the contract with you for the solution offered by us against the above RFP (Request for Proposal). We hereby extend our full warranty/support as per Conditions of Contract for the goods and services offered for supply by the above firm against this RFP (Request for Proposal).

We duly authorize the said firm to act on our behalf in fulfilling all installation, technical support and Annual maintenance obligations required by the Contract.

Yours faithfully,

(Name)

(Name of OEM)

Note: 1. This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the OEM. It should be included by the Bidder in its bid.

2. Board Resolution or equivalent corporate authorization of the manufacturer issuing the authorization shall be attached herewith.

ANNEXURE-XX Undertaking for Being OEM Proposed Product

No.

Date:

To
The General Manager,
Fraud Risk Management
Department,
2nd Floor, Uttar Pradesh Gramin
Bank
Head Office NBCC Building, Vardan Khand
Gomti Nagar Ext ext, Lucknow-226010

Sub- OEM for your RFP No.dated.....

Dear Sir

We M/s_____ are the OEM/OSD of
..... (name of product offered) do hereby
offer our quotation against the above bid invitation with our products. We hereby extend our
full warranty/support as per Conditions of Contract for the goods and services offered for supply
by the above firm against this RFP (Request for Proposal).

We hereby extend our guarantee and warranty as per the terms and conditions of this RFP
and its subsequent Corrigendum and/or Clarifications, if any, and the contract for the solution
and services offered against this invitation. In case of default/non-compliance of the software
as per RFP requirements during the contract period, we agree to replace the software supplied
with new one in accordance with RFP requirements. We also hereby undertake to perform the
obligations as set out in the RFP in fulfilling all installation, technical support and Annual
maintenance obligations required by the Contract

Yours faithfully,

Authorized Signatory

Name:
Designation:
Bidders' Corporate Name: Address:
Email and Phone

ANNEXURE XXI - Reference Site Details (per Qualifying Bank)

The reference sites submitted must be necessarily of those Banks/Companies where the OEM/OSD Bidder has been awarded the contract prior to date of issuance of this RFP and implemented in steady state.

Sites where the offered solution is accepted but implementation is not completed will not be considered. Please provide reference details in the format defined below:

Sr No	Name of Implementation/Client	
1	Successful establishment of EFRMS for Bank. The following may be given Bank wise: <ul style="list-style-type: none"> ➤ Name of the Bank/Financial Institutions ➤ Country of Operation ➤ Address of the Organization ➤ Name of the contact person for reference ➤ Phone No of contact person ➤ Email Id of contact person ➤ Designation ➤ Vertical 	
2	Project Details	
	<ul style="list-style-type: none"> ➤ Date of commencement of Project ➤ Date of Go-live/ completion of Project (if completed) ➤ Scope of Work for Solution ➤ Whether Customer profiling is in place? ➤ Whether Cross Channel Rules are in Place? ➤ Peak TPS handled by the Solution? 	
3	Whether Uttar Pradesh Gramin Bank can contact reference site to seek further information.	

(Enclose necessary documentary proof)

Place:

Date:

Signature Name & Designation:

Business Address:

ANNEXURE XXII – Know Your Employee (KYE) Clause Undertaking

(Bidder has to submit Undertaking on company letter head as per format given below).

1. We __ (name of the company) hereby confirm that all the Resource (both on-site and off-site) deployed/to be deployed on Bank's project for ____ (Name of the RFP) have undergone KYE (Know Your Employee) process and requisite checks have been performed prior to employment of said employees as per our policy.
2. We undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages, claim penalties expenses, legal liability because of non-compliance of KYE and of misconduct of the employee deployed by us to the Bank.
3. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, Educational document, credit history, etc.) to Bank before deploying officials in Bank premises for __ (Name of the RFP)."

Signature of Competent Authority with company seal

_____ Name of

Competent Authority _____

Company / Organization

Designation within Company / Organization

Date

ANNEXURE XXIII – Hardware Requirements (Sizing per Bank : DC, DR, UAT)

Date:

The General Manager
Fraud Risk Management
Department,
2nd Floor, Uttar Pradesh Gramin
Bank
Head Office, NBCC Building
Vardan Khand, Gomti Nagar Ext-226010
Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (FRM) Solution in the Bank

Ref: Your RFP No.

dated

Referring to your above RFP, we here by submit the documents covering following aspects given below:

- 1) Complete details of the hardware sizing (Data Centre, DR site, UAT/SIT), Operating system/Data Base requirements.
- 2) Network architecture of the platform offered to be submitted by the Bidder by means of Diagrammatic/ Pictorial representations.
- 3) Solution architecture including the application modules that will be provided to the Bank.
- 4) Backup and retrieval strategies and the proposed sizing requirement for the same.
- 5) Details of any other application/software that will be brought by the vendor as part of the project.
- 6) The IT Infrastructure required for hosting the proposed EFRM solution will be provided by the Bank as per Scope of the project.
- 7) If the proposed application is based on some other DB/system software, then the bidder has to provide the same with cost of such product built within the overall commercial bid/TCO.

The sizing mentioned through the submitted documents will be adequate to handle the desired TPS and Volume Projections specified as per volume projection Table in subsection 8 of section III.

For
Office Seal
Place:
Date:

(Authorised Signatory)
Name:
Designation:
Mobile No:

ANNEXURE XXIV - Work Experience Certificate (from Reference Banks)

(To Be provided in Bank's letter head)

To,

Date:

The General Manager
 Fraud Risk Management Department,
 2nd Floor, Uttar Pradesh Gramin Bank
 Head Office, NBCC Building
 Vardan Khand, Gomti Nagar Ext-226010

Dear Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Management and Maintenance of Enterprise Fraud Risk Management (EFRM) Solution in the Bank

Ref: Your RFP No. GEM/ dated

This is to certify that M/s (Name of Vendor) has supplied and implemented the EFRM solution (Name of EFRM solution), covering (No of Branches) Branches across the Bank since (Year of implementation).

The EFRM solution Implemented covers the following channels/Switches in Preventive Real Time mode and at an Enterprise level as on 31.03.2025:

SI No	Channel	Yes	No
1	UPI Outward		
2	UPI Inward		
3	Internet Banking (Retail)		
4	Internet Banking (Corporate)		
5	Mobile Banking (Retail)		
6	Mobile Banking (Corporate)		
7	IMPS Inward		
8	IMPS Outward		
9	Credit Card		
10	Debit Card (ATM Switch)		
11	AEPS		
12	NEFT & RTGS (Inward)		
13	NEFT & RTGS (Outward)		
14	Branch Transactions		
15	CBDC		

Signature of Authorized Official

Name and Designation with Office Seal

Place & date:

ANNEXURE XXV - Undertaking for Product Presentation, Demonstration and Implementation Readiness

No.

Date:

To
The General Manager,
Fraud Risk Management Department,
2nd Floor, NBCC building, Vardan Khand,
Lucknow-226010

Sub- RFP No.dated.....

Dear Sir,

We, [Vendor Name / OEM Name], hereby undertake that:

6. The product features, functionalities, and capabilities showcased during the Product Presentation and Demonstration of [Product Name] on [Date] have already been implemented and are LIVE in production in at least two banks: [Bank Name 1] having [_____] branches and [Bank Name 2] having [_____] branches as on 31.03.2026.
7. All demonstrated features are currently available in the production version of the solution and are NOT planned future features or features under development.
8. During site visits and reference checks by UPGB and GGB officials, the above claims may be verified. If our claims are found incorrect or misleading, both Banks are authorised to: (a) recalibrate the technical scores awarded to us; (b) disqualify our bid; and/or (c) debar us from future tenders.
9. The demonstrated solution is production-ready and fully deployable at both UPGB and GGB, and we shall ensure delivery, installation, and implementation of the same in the live environments of both Banks within the timelines specified in this RFP.

For

Office Seal

Place:

Date:

(Authorised Signatory)

Name:

Designation:

Mobile No:

Business Address:

Telephone

**Annexure XXVI –Details of Hardware, OS & DB Requirement
(Separately for UPGB and GGB)**

RFP No.

Date:

To
The General Manager,
Fraud Risk Management Department,
2nd Floor, NBCC building, Vardan Khand,
Lucknow-226010

The Bidder must specify complete details of Hardware and other systems required for successful implementation of the offered Solution, in the following format.

Sr. No.	Module/ Item	Module Description	Requirement	Quantity
1	Hardware - Bank's on premise cloud infrastructure (Processor core and speed, RAM, HDD, etc.)			
2	Hardware - Bank's on premise cloud infrastructure (Processor core and speed, RAM, HDD, etc.)			
3	Database			

Note:

Please mention Make / Model (if any), type and number of processors, Memory, bus speed, hard disk & Operating System number of users, license type, version etc.

- The resource including CPU utilization of any server/ appliance should not go beyond 70%. If the same crosses the threshold of 70% five times in a day or 10 times in a week, bidder should fine tune the application to ensure the utilization within the aforesaid threshold without any additional cost to the bank.

For

Office Seal

Place:

Date:

(Authorised Signatory)

Name:

Designation:

Mobile No:

Business Address:

Annexure XXVII –Data Security and Segregation Compliance Undertaking

(To be submitted on Bidder’s and OEM’s letterhead, signed by respective Authorised Signatories)

RFP No.

Date:

To
 The General Manager,
 Fraud Risk Management Department,
 2nd Floor, NBCC building, Vardan Khand,
 Lucknow-226010

We, M/s _____ (Bidder) and M/s _____ (OEM, if different), hereby jointly and severally undertake that:

1. The EFRM Solution deployed for Uttar Pradesh Gramin Bank (UPGB) and Gujarat Gramin Bank (GGB) will be physically and logically COMPLETELY SEGREGATED. No data of UPGB – including transaction data, customer data, case data, alert data, audit logs, device intelligence data, and behavioural biometric data – will at any time be accessible to or visible in the GGB deployment, and vice versa.
2. We will conduct an independent security audit of the data segregation architecture of both Banks’ deployments and provide written certification to both Banks before Phase 1 Go-Live.
3. Resources deployed for UPGB implementation and operations will not have access to GGB’s systems, databases, or data. Separate user access management will be maintained for each Bank’s environment.
4. All customer data, transaction data, and related information of each Bank will be stored exclusively within that Bank’s own IT infrastructure within India. Cross-border data transfer is absolutely prohibited.
5. In the event of a data segregation breach, we will immediately notify both Banks, take corrective action at no cost, and submit a Root Cause Analysis and remediation plan within 48 hours.
6. We acknowledge that any data segregation breach constitutes a material contract violation entitling the affected Bank to terminate the contract and invoke the Performance Bank Guarantee.

Bidder Authorised Signatory	OEM Authorised Signatory (if different)
Name & Designation:	Name & Designation:
Company Seal	OEM Seal
Date & Place:	Date & Place: