Request for Proposal
for
Supply, Installation, Implementation, Integration, Training
and
Maintenance of Fraud Risk Management System

Customization Department CDO Vertical

HEAD OFFICE

NAINITAL

The Nainital Bank Limited

21st March, 2025

RFP Reference No- **NTB/IT/FRMS/2025/03/023**

Contents

List of Abbreviations

Acronym	Full Form
AMC	Annual Maintenance Contract
BG	Bank Guarantee
CBS	Core Banking Solution
DC	Data Centre
DD / PO	Demand Draft / Pay Order
DR	Disaster Recovery
EOD	End of Day
BOD	Begin of Day
EMD	Earnest Money Deposit
IT	Information Technology
JSON	JavaScript Object Notation
LoI	Letter of Intent
MIS	Management Information Systems
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
OSD	Original Software Developer
PBG	Performance Bank Guarantee
PO	Purchase Order
RBI	Reserve Bank of India
RFP	Request for Proposal
SLA	Service Level Agreement
TCO	Total cost to Ownership
TO	Technical Offer
XML	Extensible Markup Language
TS	Marks obtained for Technical Proposal

1. Section I – Invitation to Bid

RFP No. NTB/IT/FRMS/2025/03/023

The Nainital Bank Ltd.

Head Office,

Seven Oaks Building,

Mallital, Nainital, Uttarakhand - 263001

Dated: 21/03/2025

The Nainital Bank Ltd. invites bids (Technical & Financial) from eligible bidders which are valid for a period of 180 days from the last date of submission of bid.

Scope of Work	**Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System**	
Application Money	**Rs. 20,000/- (Rupees Twenty Thousands Only)**	Application money has to be deposited in the form of DD/PO/NEFT* at the time of submission of Bid.
EMD (Earnest Money Deposit) to be submitted	**Rs. 5,00,000/- (Rupees Five Lakhs Only)**	Earnest Money Deposit (EMD) submitted in the form of DD/PO /NEFT or Bank Guarantee which should be valid for a period of 6 months from the last date of bid submission date. EMD to be deposited along with the bid.
Date of issue of RFP		21st March, 2025
Last date and time of submission of Bids		10/04/2025 (1600 Hrs)
Date and time of opening of Eligibility cum Technical Bids (envelope 1 and envelope 2)		Date and time of opening of envelope 1 & 2 will be shared later to the bidders (through the authorized e-mail IDs shared by the bidders in the Bidder Profile.)

Interested parties may view and download the RFP Document containing the detailed terms & conditions, from the website https://www.nainitalbank.co.in/english/tender.aspx

***DD/PO/NEFT and Bank Guarantee should be made in the favour of The Nainital Bank Ltd. and DD/PO to be made Payable at Delhi.**

1.1. Document Control Sheet

RFP Reference No.	**NTB/IT/FRMS/2025/03/023**
Name of Organization	The Nainital Bank Limited
RFP Type (Open/Limited/EOI/Auction/Single)	Open
RFP Category (Services/Goods/works)	Services/Goods
Type/Form of Contract (Work/Supply/Auction/Service/ Buy/ Empanelment/Sell)	Work/Service/Buy
Technical Evaluation (Yes/No)	Yes
Is Multi Currency Allowed	No (Only INR)
Payment Mode (Online/Offline)	Online/Offline
RFP Issuance Date	21/03/2025
RFP Coordinator	RFP Coordinator – Rohina Ruqaiya Ahmad, IT Officer Contact No. – +91-9084719037 E-mail – customization@nainitalbank.co.in
Last date of receiving written request for clarifications before the pre-bid meeting	13:00 hrs on 26th March, 2025 E-mail: customization@nainitalbank.co.in
Pre-bid meeting	• Pre bid meeting will be held through online mode on 28/03/2025 between 3.30 PM and 05:00 PM. • Bidder to submit the names of -2- authorized officials/persons (Maximum) along with their contact numbers, designations and email IDs on customization@nainitalbank.co.in by 13:00 hrs on 26/03/2025 along with the clarification sought (if any) in the format prescribed in point 2.8. • Invitation link of the meeting will be sent by the Bank to the email IDs (max. 2) of authorized officials/persons of the bidder to join the Online Pre-Bid Meeting as per the schedule mentioned above. • In order to join the On-Line Pre-bid meeting, the Bidder's representatives will have to click the link provided through E-mail by the Bank.

Last date of submission of RFP response (Closing date) and address for submission of Bid	16:00 Hrs. on 10/04/2025 at The Nainital Bank Ltd., Customization Dept., CDO Vertical, Head Office, Seven Oaks Building, Mallital, Nainital, Uttarakhand – 263001
Mode of Submission of Bid	The Bidder shall send the Bid Envelope through Courier / Registered Post / Speed Post or deposit the Bid envelope in person in the tender/RFP box kept for this purpose at **The Nainital Bank Ltd., Customization Dept., CDO Vertical, Head Office, Seven Oaks Building, Mallital, Nainital, Uttarakhand – 263001** on or before 16:00 hrs on 10/04/2025 (Bid Submission Date & Time). The date of dispatch of Courier / Registered Post / Speed Post receipt should be on or before the last date of bid submission. The receipt of Courier / Registered Post / Speed Post for tracking purposes should be sent on the email id of RFP Coordinator mentioned in the Document Control Sheet. However, if the said Bid Envelope dispatched before the last date of bid submission, sent through Courier / Registered Post / Speed Post is lost in transit or is not delivered within 7 days from the last date of bid submission in such circumstances the Bank shall not be liable, whatsoever, due to such misplacement or non-delivery of the said bid envelope. Further, the Bidder, whose bid envelope is misplaced in transit or is undelivered within 7 days from the last date of bid submission cannot resubmit his bid on the pretext of lost in transit, misplacement or non-delivery of the Bid envelope.
Date and time of opening of Eligibility Cum Technical Bids (envelope 1 and envelope 2)	Date and time of the opening of envelope 1 & 2 will be shared later to the bidders (through the authorized e-mail IDs shared by the bidders).

Date of Technical Presentation	Date of technical presentation will be shared later to the eligible bidders through authorized e-mail ID shared by the bidders.
Contract Type (Empanelment/RFP)	RFP
Multiple Technical Annexure(s)	Yes
Quoting for all Technical Annexures is compulsory	Yes
Application money*	Application Money of Rs. 20,000/- (Rupees Twenty Thousand Only) has to be deposited in the form of DD / PO / NEFT at the time of Bid submission. The NEFT should be sent on or before last date of Bid submission as per account details mentioned below: Account Name – APPLICATION MONEY & EMD Account Number - 999421390000001 IFSC Code - NTBL0NAI999 Branch Name - Head Office, Nainital
Bid Security (Earnest Money Deposit)	EMD of Rs. 5,00,000/- (Rupees Five Lakhs Only) submitted in the form of DD/PO/NEFT or Bank Guarantee which should be valid for a period of -6-(six) months from the last date for bid submission date. EMD to be deposited along with the bid. The NEFT should be sent on or before revised last date of Bid submission as per account details mentioned below: Account Name - APPLICATION MONEY & EMD Account Number - 999421390000001 IFSC Code - NTBL0NAI999 Branch Name - Head Office, Nainital
Bid Validity days	180 days from the last date of submission of bid
Location for Submission of Bid	**The Nainital Bank Ltd.,** **Customization Dept., CDO Vertical,** **Head Office,** **Seven Oaks Building,** **Mallital, Nainital, Uttarakhand – 263001**
Validity of Contract	5 years initially from the date of Go-Live of the application, extendable for a period of 3 years solely at the discretion of the Bank.

Address for Communication	Mr. Gaurava Kumar Sharma, Chief Digital Officer, Customization Department CDO Vertical, The Nainital Bank Ltd., Head Office, Seven Oaks Building, Mallital, Nainital, Uttarakhand - 263001

MSEs (Micro and Small Enterprise (MSE) are exempted from paying the application money and Bid security amount for which the concerned enterprise needs to provide necessary documentary evidence. For MSEs Government of India provisions shall be considered while evaluating the RFP. (Please refer Pt. 2.6 of this RFP document for detailing the MSE clause)
*DD/PO/NEFT and Bank Guarantee should be made in the favour of The Nainital Bank Ltd..

1.2. DISCLAIMER

The information contained in this Request for Proposal Document (RFP Document) or subsequently provided to Bidder/s, whether verbally or in documentary form by or on behalf of the Nainital Bank Limited or any of their representatives, employees or advisors (collectively referred to as — Bank Representatives), is provided to Bidder(s) on the terms and conditions set out in this RFP Document and any other terms and conditions subject to which such information is provided. This document shall not be transferred, reproduced, or otherwise used for purpose other than for which it is specifically issued.
This RFP Document is not an agreement and is not an offer or invitation by the Bank Representatives to any party other than the entities who are qualified to submit their Proposal (Bidders). The purpose of this RFP Document is to provide the Bidder with information to assist the formulation of their Proposal. This RFP Document does not purport to contain all the information each Bidder may require. This RFP Document may not be appropriate for all persons, and it is not possible for the Bank Representatives, their employees, or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP Document.
The Bank, its employees and advisors make no representation and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form or arising in any way for participation in this bidding process. The Bank also accepts no liability of any nature whether resulting from negligence or otherwise, howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. The Bidder is expected to examine all instructions, forms, terms and specifications in the bidding Document. Failure to furnish all information required by the bidding Document or to submit a Bid not substantially responsive to the bidding Document in all respect will be at the Bidder's risk and may result in rejection of the Bid. The Bank Representatives may in their absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP Document.
Subject to any law to the contrary and to the maximum extent permitted by law, the Bank and its Directors, Officers, employees, contractors, representatives, agents and advisors disclaim all liability from

any loss, claim, expenses (including, without limitation, any legal fees, costs, charges, demands, actions, liabilities, expenses or disbursement incurred therein or incidental thereto) or damage, (whether foreseeable or not) ("losses") suffered by any person acting on or refraining from acting because of any presumption or information(whether oral or written and whether expressed or implied), including forecasts, statements, estimate or projections contained in this RFP document or conduct ancillary to it whether or not the losses rise in connection with any ignorance, negligence, inattention, casualness, disregard, omission, default, lack of care, immature information, falsification or misrepresentation on the part of the Bank or any of its Directors, officers, employees, contractors, representatives, agents, or advisors.

2. Section II: Instructions for Bid Submission

2.1. Executive summary of the project

The Nainital Bank Limited was established in the year 1922 with the objective to cater to the banking needs of the people of the region. Bank of Baroda, a premier nationalized bank, is managing the affairs of The Nainital Bank Limited since 1973. At present, the Bank is operating in five states i.e. Uttarakhand, Uttar Pradesh, Delhi, Haryana and Rajasthan, having 173 branches which may however increase in future consequent to opening of new branches. The bank's Head Office is at Nainital, Uttarakhand and its -3- Regional Offices are functioning at Delhi, Dehradun and Haldwani. The Bank is running with a vision which states: "To emerge as a customer centric National Bank & become the most preferred bank for its product, services, technology, efficiency & financials."

The Nainital Bank Ltd has strategic plans to enhance the various banking delivery channels and integrate them in a way, to deliver seamless and superior digital experience to the customers and stakeholders. Technology has enabled the delivery of banking services through multiple channels, improving convenience, reach and speed.

With the increase in the digital channels for payments and thereby the rapid growth in number of digital payments, The Nainital Bank Ltd has strategic plans to enhance the security of the payments of the banks' customers by implementing a seamless and superior digital experience with robust fraud prevention. The bank aims to integrate fraud prevention with regulatory compliance while also preventing data breaches.

2.2. Preparation of Bids

Bidder should consider all corrigendum/s, (if any), published on the Bank's website related to the RFP Document before submitting their bids.

Please go through the advertisement and the RFP Document carefully to understand the documents required to be submitted as part of the bid. Please note the number of cover envelopes in which the bid documents have to be submitted, the number of documents - including the names and contents of each of the document that needs to be submitted. Any deviations from these may lead to rejection of the bid.

2.3. Submission of Bids

The bidder shall submit all Pre-qualification documents in an envelope which will be marked as **"Envelope No. 1: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System - Pre-Qualification Envelope".**

The Bidder shall seal the original DD/PO or Bank Guarantee as EMD and Application fees in the form of DD/PO in this Envelope No. 1 along with other Pre-qualification documents. If the same are deposited through NEFT, as the case may be, details of the same should be submitted in the Bidder's Profile as mentioned in **section V point no. 5.1**. The Bidder shall mark its company/firm/LLP name and RFP reference number on the back of the Bank Demand Draft/PO before sealing the same.

One paper copy and one electronic copy (Power Point or Microsoft Word and Excel contained in storage media) of all documents submitted under Technical Bid (Envelope No. 2) must be submitted to the Bank

and addressed as **"Envelope No. 2: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System – Technical Bid Envelope".**

The bidder shall submit all documents containing commercial bids (**Refer Annexure-15 - Commercial Bid Format)** in an envelope which will be marked as "**Envelope No. 3: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System – Commercial Bid Envelope".**

The Bidder shall send the Bid Envelopes through Courier / Registered Post / Speed Post or deposit the Bid envelopes in person in the RFP box kept for this purpose at The Nainital Bank Ltd., Customization Dept, CDO Vertical, Head Office, Seven Oaks building, Mallital, Nainital, Uttarakhand – 263001 on or before 1600 Hrs 10/04/2025 (Bid Submission Date).

The date of dispatch of Courier / Registered Post / Speed Post receipt should be on or before the last date of bid submission. The receipt of Courier / Registered Post / Speed Post for tracking purposes should be sent on the email id of the RFP Coordinator mentioned in the Document Control Sheet.
However, if the said Bid Envelopes sent through Courier / Registered Post / Speed Post are lost in transit or are not delivered within 7 days from the last date of bid submission, in such circumstances, the Bank shall not be liable, whatsoever, due to such loss in transit, misplacement or non-delivery of the said bid envelopes.

Further, the Bidder, whose bid envelopes are lost in transit, misplaced in transit or are undelivered within 7 days from the last date of bid submission cannot resubmit his bid on the pretext of lost in transit, misplacement or non-delivery of the Bid envelopes.

Documents Comprising the Bids

1. **Envelope 1 - <u>Pre Qualification envelope</u>**

The Pre-qualification envelope, besides the other requirements of the RFP, shall comprise of the following: (The envelope should be marked as "**Envelope No. 1: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System - Pre-Qualification Envelope"**). Bidder has to provide all documents mentioned in **Annexure 01 – Eligibility Bid - Table of Contents (list of document enclosed).**

2. **Envelope 2 - <u>Technical Bid envelope</u>**

The Technical Bid, besides the other requirements of the RFP, shall comprise of the following: (The envelope should be marked as "**Envelope No. 2: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System – Technical bid envelope**")

- Index
- Technical Bid Letter
- Technical / Functional Specifications (Refer Annexure 11- Technical requirement (Broad Scope of Work))

- Technical Specifications compliance separately in each requirement given in **Table 6 Technical Score in Annexure 11.**
- Detailed approach & methodology for providing the proposed service (Refer Point 2.32 Technical Presentation of Evaluation of Technical Bids)
- Supporting documents as required in technical score sheet
- All documents including Power point presentation, technical compliance in a storage media. Technical compliance has to be submitted in excel format.
  All documents should be signed and stamped (manual or digital) by the authorized person.
- Undertaking by the Bidder to be submitted in format mentioned at **Section V Point 5.4**
- Executive Technical Summary **Annexure 18**

3. Envelope 3 - Commercial Bid envelope

The Commercial Bid, besides the other requirements of the RFP, shall comprise of the following: (The envelope should be marked as "**Envelope No. 3: Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System – Commercial Bid Envelope**")

Commercial Bid envelope to contain the following

Section #	Section Heading	Pro forma Given
1	Covering letter on submission of Commercial Bid	**Bidder to provide**
2	Conformity with Hard Copy	**Annexure 07**
3	Commercial Bid	**Annexure 15**

A standard format for submission of commercial bids has been provided with the RFP to be filled by all the bidders. Bidders are requested to note that they should necessarily submit their commercial bids in the format provided in **Annexure 15** (Commercial Bid Format) and submission in any other format will lead to rejection of the bid.

2.4. Assistance to Bidders

Any queries relating to the RFP Document and the terms and conditions contained therein should be addressed to the RFP Coordinator indicated in this RFP.

2.5. Cost to Bid

The Bidder shall bear all costs associated with the preparation and submission of its bid, including cost of presentation for the purposes of clarification of the bid or otherwise. The Bank, will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the RFP process.

2.6. Micro and Small Enterprise (MSE)

As per recommendations of GOI (Government of India), Bank has decided to waive off EMD, tender/RFP

cost (application money) and, Fees for proposed solution features for Micro and Small Enterprise MSE.

i. MSEs are exempted from paying the application money and Bid security amount for which the concerned enterprise needs to provide necessary documentary evidence issued by NSIC (National Small Industries Corporation). For MSEs Government of India provisions shall be considered while evaluating the tender/RFP. Bids received without EMD, tender/RFP cost (application money), and Fees for proposed solution features from Bidders not having valid NSIC (National Small Industries Corporation) registered documents for exemption will not be considered.
ii. To qualify for EMD, Tender/RFP Fee / Cost (application fee), and Fees for proposed solution features exemption, firms should necessarily enclose a valid copy of registration certificate which is valid on last date of submission of the tender/RFP documents. MSE firms who are in the process of obtaining registration will not be considered for EMD, Tender/RFP Fee / Cost (application fee), and Fees for proposed solution features exemption.
iii. MSE Bidder has to submit a self-declaration accepting that if they are awarded the contract and they fail to sign the contract or to submit a Performance Bank Guarantee before the deadline defined by the Bank, they will be suspended for a period of three years from being eligible to submit bids for contracts with the Bank.
iv. Bids received without EMD for Bidders not having valid registration documents for exemption will not be considered. However, Performance Bank Guarantee has to be submitted by the Bidder under any circumstance.
v. The Udyam Registration Certificate (URC) submitted as proof of MSE should be valid as on the last date of submission of the RFP. The NIC codes mentioned in the URC should mention the services currently rendered by the bidder.

2.7. Contents of the RFP Document

The RFP Document is divided into following sections:

1. Section I - Invitation for Bids
2. Section II - Instructions for Bid submission
3. Section III - Detailed Scope of Work
4. Section IV - General Conditions of the Contract and Service Level Agreement
5. Section V - Bid Submission Format
6. Section VI - Annexure

The Bidder is expected to examine all instructions, forms, terms & conditions, and scope of work in the RFP Document and furnish all information as stipulated therein.

2.8. Clarification on RFP Document

A prospective Bidder requiring any clarification on the RFP Document may submit his/her queries, through email, at the Bank's e-mail address i.e. **customization@nainitalbank.co.in** and as per schedule indicated under **point no. 1.1 of Section I – Invitation for Bids.** The queries must be submitted in the following format (in Excel file, *.xls) shall only be considered for clarification:

Sr. No	Page No./ Section No.	Clause No.	Reference/ Subject	Clarification Sought
..	..	..	..	..

The Bank will only respond to queries submitted in the above excel format.

All queries on the RFP Document should be received on or before the last date and time as prescribed by the Bank in Section I of this RFP Document. Bank's response (including the query but without identifying the source of inquiry) would be provided to the bidders present during the Pre-bid meeting and corrigendum (if any) would be uploaded on bank's website https://www.nainitalbank.co.in/english/tender.aspx. Bidders are responsible for duly checking the above website for any clarification(s)/ corrigendum(s) and Bank's response.

Note: Inputs/suggestions/queries submitted by bidders as part of the pre-bid queries and otherwise will be given due consideration by the Bank, however THE NAINITAL BANK LTD. is not mandated to accept any submission made by the bidder and nor the bidder will be given any written response to their submissions. If an input is considered valid by the Bank the same will be accepted and incorporated as part of the corrigendum and shall be published on Bank's website.

2.9. Amendment of RFP Document

At any time prior to the last date for receipt of bids, the Bank, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by an amendment. Amendments, if any will be notified in writing on bank's website www.nainitalbank.co.in under Tender Section and shall be binding on all bidders. In order to provide prospective Bidders with a reasonable time, to take the amendment into account in preparing their bids, the Bank may, at its discretion, extend the last date for the receipt of Bids. Any or all corrigendum/amendments notified by the Bank shall be treated as an integral part of this RFP.

2.10. Language of Bids

The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Bank, shall be written in **English language.**

2.11. Bid Prices

The Bidder shall indicate in the pro forma prescribed in Section VI Annexure 15 (Commercial Bid Format), the total Bid Prices of the services it proposes to provide under the Contract. Prices should be shown separately for each item as detailed in RFP Documents.

In the absence of above information as requested, a bid may be considered incomplete and be summarily rejected.

The Bidder shall prepare the bid based on details provided in the RFP Documents. It must be clearly understood that the Scope of Work (as indicated in Section VI Annexure-11 Detailed Scope of Work) is intended to give the Bidder an idea about the order and magnitude of the work / solution required by the Bank and is not in any way exhaustive and guaranteed by the Bank. The Bidder shall carry out all the tasks in accordance with the requirement of the RFP Documents and it shall be the responsibility of the Bidder

to fully meet all the requirements of the RFP Documents.

2.12. Firm Prices

Prices quoted in the bid must be firm and final and shall not be subject to any upward modifications, on any account whatsoever. However, the Bank reserves the right to negotiate the prices quoted in the bid to effect downward modification. The Bid Prices shall be indicated in Indian Rupees (INR) only.
The Financial bid should clearly indicate the price to be charged and Taxes will be applicable as per actuals. It is mandatory that such charges wherever applicable/payable should be indicated separately in **Section V – Bid Submission Format**. However, should there be a change in the applicable taxes, the same may apply.

2.13. Bidder Qualification

The "Bidder" as used in the RFP Documents shall mean the one who has signed the RFP Form. The Bidder may be either the **Principal Officer** or his duly **Authorized Representative**, in either cases he/she shall submit a certificate of authority. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall, as far as possible, be furnished and signed by the representative and the principal Officer.
It is further clarified that the individual signing the RFP or other documents in connection with the RFP must certify whether he/she signs as the Constituted attorney of the firm, or of the company.
The authorization shall be indicated by **written power-of-attorney** or latest Board Resolution in case of company authorizing the Principal Officer / Authorized representative accompanying the bid.
The power of attorney and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder shall be annexed to the bid.
Any change in the Principal Officer shall be intimated to THE NAINITAL BANK LTD. in advance.

2.14. Earnest Money Deposit (EMD)

The Bidder shall furnish, as part of its bid, an Earnest Money Deposit (EMD) of the amount Rs. 5,00,000/- (Rupees Five Lakhs Only) as per details in the Document Control Sheet as a security.
The EMD is required to protect the Bank against the risk of Bidder's conduct which would warrant the security's forfeiture.
The EMD must be submitted, in form of DD/PO or Bank Guarantee valid for a period of -6- months from the last date of bid submission, of any Scheduled Commercial Bank (except of the Nainital Bank Ltd.) favouring The Nainital Bank Ltd. In case the EMD is sent through NEFT, such details are to be submitted as mentioned at **Section V clause 5.1**
In case of bidders being an MSE under registration of any scheme of Ministry of MSE, they are exempted from the submission of EMD. A valid certificate in this regard issued by the NSIC has to be submitted along with the bid. (Please refer **Section II clause 2.6** Micro and Small Enterprises clause for details)
Unsuccessful Bidder's EMD will be returned after the bank sends the pro forma of the contract to the successful Bidder. **No interest will be paid by the Bank on the EMD**.
The successful Bidder's EMD will be discharged upon the bidder executing the Contract, and furnishing the Bank Guarantee/security deposit. **No interest will be paid by the Bank on the EMD.**
The EMD may be forfeited:

a. if a Bidder withdraws its bid during the period of bid validity specified in the RFP; or
b. in the case of a successful Bidder, if the Bidder fails;
   I. To sign the Contract/SLA in accordance; or
   ii. To furnish Security Deposit/Bank Guarantee for contract performance.
   iii. To comply with any other condition precedent to signing the contract specified in the RFP documents.

2.15. Security Deposit/Performance Guarantee:

The successful bidder will be required to submit Security deposit in the form of Bank Guarantee, favouring The Nainital Bank Ltd. equal to the 10% of purchase order value for the entire period of contract i.e. 60 months and such other extended period as the Bank may decide for due performance of the project obligations. The Guarantee should be issued from any Schedule Commercial Bank Only, other than Nainital Bank Ltd.

In the event of non-performance of obligation or failure to meet terms of this RFP or subsequent agreement the Bank shall be entitled to appropriate/invoke the security Deposits/Performance Bank Guarantee as the case may be without notice or right of demur to the Bidder.

The Bank reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected Bidder, including the pending bills and/or invoking Guarantee, if any, under the agreement.

Validity: The term of this Contract will commence from the date of signing of contract/agreement and will be valid for a period of five (5) years which will be computed from the date of Go-Live of proposed solution. (Apart from above said 5 years' term, both Bank and Bidder shall also be governed by the terms of the said agreement for the term of preparation period i.e. the period between date of signing of agreement till date of go-live of solution). The contract is extendable further for three (3) years solely at the discretion of the Bank.

The BG will be released after 6 months and/or extended period or execution of all pending Orders, whichever is later.

In the event of termination, Bank may invoke the Performance Bank Guarantee/Security Deposits, recover such other direct costs and other amount towards direct damages from the successful bidder that may have resulted from such default and pursue such other rights and/or remedies that may be available to the Bank under law.

2.16. Period of Validity of Bids

Validity of bid will be 180 days from the last date of submission of bid. **Any bid of a shorter period may be rejected by the Bank as non- responsive.**

In exceptional circumstances, the Bank may request the Bidder(s) for an extension of the period of validity of bids up to 180 days. Any clarification/request or response thereto on extension of period of bid submission or extension of period of validity of EMD shall be done as per this RFP document. The validity of EMD may also be extended if required subject to approval of the bank's committee in charge of the RFP process.

2.17. Format and Signing of Bid

The original and all copies of the bid shall be typed or written in indelible ink. **The original and all copies** shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Agreement/Contract. All pages of the bid, except for un-amended printed literature, shall be initialled or digitally signed and stamped by the person or persons signing the bid.

The response to the bid should be submitted along with legible, appropriately indexed, duly filled information sheets and sufficient documentary evidence as per Checklist. Responses with illegible, incomplete information sheets or insufficient documentary evidence shall be rejected.

The Bidder shall duly sign (manual or digital) and seal its bid with the exact name of the firm/company/LLP to whom the contract/agreement is to be issued.

2.18. Revelation of Prices

Prices in any form or by any reason before opening the Commercial/Financial Bid should not be revealed, failing which the offer shall be liable to be rejected.

2.19. Terms and Conditions of Bidders

Printed terms and conditions of the Bidders will not be considered as forming part of their Bids. The terms and conditions mentioned the RFP will solely prevail.

2.20. Consortium

Consortium is not allowed.

2.21. Sub- Contracting:

The selected bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required under this project. In case any particular specialized service prescribed in the scope of work requires subcontracting, it needs to be specified in the proposal/ response document with all the details of the work/ services. Please note that no work/services shall be subcontracted without the prior permission from the Bank in writing.

2.22. Last Date & Time for Receipt of Bids

Bids will be received by the Bank at the address specified under Section I - Invitation for Bids no later than the time and date specified in Section I -Invitation for Bids.

The Bank may, at its discretion, extend the last date for the receipt of bids by amending the RFP Document, in which case all rights and obligations of the Bank and Bidders previously subject to the last date will thereafter be subject to the last date as extended.

2.23. Late Bids

Any bid received by the Bank after the last date and time for receipt of bids prescribed by the Bank, pursuant to **Section I - Invitation for Bids, shall stand rejected.**

2.24. Modification and Withdrawal of Bids

No bid may be altered / modified subsequent to the closing time and date for receipt of bids. Unsolicited correspondences from Bidders will not be considered.

No bid may be withdrawn in the interval between the date for receipt of bids and the expiry of the bid validity period specified by the Bidder in the Bid. Withdrawal of a bid during this interval may result in the Bidder's forfeiture of its EMD.

2.25. Bidder's Address for Correspondence

The Bidder shall designate the official mailing address, place to which all correspondence shall be sent by the Bank.

2.26. Contacting the Bank

No Bidder shall contact the Bank on any matter relating to its bid, from the time of the bid opening up to the time of award of contract.

Any effort by a Bidder to influence the Bank's bid evaluation, bid comparison or contract award decisions may result in the rejection of the Bidder's bid.

2.27. Opening of Bids by Bank

The Bank will convene a bid opening session as per time schedule where one representative from the Bidder, who has successfully submitted the bid, may participate. Subsequent to this, Bank will further evaluate the Bid of only those agencies whose Application fees, EMD and eligibility criteria is found to be in order.

2.28. Evaluation of Bids

Bank will evaluate the bids. Decision of the Bank would be final and binding upon all the Bidders.

The purpose of this clause is only to provide the Bidders an idea/overview of the evaluation process that the Bank may adopt. However, the Bank reserves the right to modify the evaluation process at any time during the RFP process, without assigning any reason, whatsoever, and without any requirement of intimating the Bidders of any such change.

Bidder must possess the requisite experience, strength and capabilities in providing the Services/ solution necessary to meet the Bank's requirements, as described in the RFP Document. Bidder must possess the technical know-how and the commercial wherewithal that would be required to successfully deliver the services, to provide the maintenance and management support services sought by the Bank, for the entire period of the agreement/contract. The Bidder's bid must be completed in all respect and covering the entire scope of work as stipulated in the RFP Document.

2.29. Preliminary Examination

The Bank will examine the bids to determine whether they are complete, whether the bid format conforms to the RFP requirements, whether any computational errors have been made, whether required EMD have been furnished, whether the documents have been properly signed (manually or digitally), and whether the bids are generally in order.

A bid determined as not substantially responsive will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.

2.30. Clarification

When deemed necessary, during the RFP process, the Bank may seek clarifications or ask the Bidders to make Technical presentations on any aspect from any or all the Bidders. However, that would not entitle the Bidder to change or cause any change in the substance of the RFP submitted or price quoted.
THE NAINITAL BANK LTD. reserves the right to seek fresh set of documents or seek clarifications on the already submitted documents.

2.31. Evaluation of Eligibility Criteria

In this part, the bid will be reviewed for determining the compliance of the general conditions of the contract and Eligibility Criteria as mentioned in the RFP. Any deviation from general conditions of the contract/agreement and eligibility criteria will lead to rejection of the bid.

Before opening and evaluation of the technical proposals, bidders are expected to meet all the general conditions of the contract and the eligibility criteria as mentioned below. Bidders failing to meet these criteria or not submitting requisite supporting documents / documentary evidence for supporting pre-qualification criteria are liable to be rejected summarily.

The bidder must possess the requisite experience, strength and capabilities in providing the solution necessary to meet the requirements, as described in the RFP Document. The bidder must also possess the technical knowhow and the commercial wherewithal that would be required to successfully provide the support services sought by THE NAINITAL BANK LTD. for the entire period of the agreement/contract. The bids must be complete in all respects and should cover the entire scope of work as stipulated in the RFP Document.

The invitation to the bids is open to all bidders who qualify the eligibility criteria as mentioned in **Annexure 01 – Eligibility Bid - Table of Contents (list of document enclosed).**

2.32. Evaluation of Technical Bid

Only those bidders who qualify all Pre-qualification / Eligibility Criteria requirements will be qualified for technical bid evaluation. Technical presentation, will also be a part of the process for evaluation of the bids. The Bank reserves the right to reject a service if it is of the opinion that the offered service does not match the technical requirements /objectives specified in Technical Bid – Bank's Requirements. The technical bid will first be reviewed for determining the Compliance of the Technical bids with the RFP terms and conditions, Minimum/Mandatory Technical requirements and the scope of work as defined in this RFP.
Any bid found to be non-compliant to the mandatory Technical Requirements, RFP terms and conditions and the scope of work shall be rejected and will not be considered for further evaluation.
The vendor needs to achieve a cut – off score of 70 marks in this evaluation stage to be qualified for commercial bid opening. Only those vendors who achieve the specified cut – off scores would be short-listed for Commercial Bid Evaluation. Further the vendor must score a minimum of 80% compliance in Technical Specifications compliance separately in each requirement given in **Table 6 Technical Score in**

annexure 11 (0.20 Mark for Each Points, Total 300 points having 60 marks). Even if the vendor meets the 70-mark cut-off and does not meet this criterion of 80% compliance in the requirement table mentioned in Annexure 11 (Table 6), the vendor would have deemed not to be meeting the RFP Technical requirements. The Technical Proposal will be evaluated for technical suitability and the criteria for evaluation of technical bids are as under:

Criteria	Evaluation Parameters	Sub Scores
The number of Implementations carried out in India in the last 5 years starting from 01-04-2020 till RFP submission date **	For each Implementation 2 marks maximum up to 10 marks	10
	Additional Marks for implementation in any Banking / Financial / Insurance Sector in India / Globally. Proof of such work and completion of implementation should be submitted along with the response.	
Technical Specifications compliance	As per Technical Scoring Sheet in Annexure 11 (Table 6)	60
Technical Presentation on Proposed Solution by the Bidder	Technical presentation will be evaluated on the following parameters: 1. Proposed Solution (6 Marks) 2. IT architecture and approach & methodology (6 Marks) 3. Resource Planning (6 Marks) 4. Project Governance and Project Team (6 Marks) 5. Future Scalability (6 Marks)	30
TOTAL MARKS		**100**

**Copies of Work order / client reference should be provided. Documentary proof for go live of implementation to be provided.

Site Visit and Reference checks

All eligible bidders will be required to arrange a Site Visit and Reference checks for the Bank's Team in a Scheduled Public/Private Sector Bank in India with at least 200 branches where the proposed solution is implemented. The format for reference check is as per **Annexure-14**

Further the Bank's officials would visit reference sites provided by the Vendor if deemed necessary.

In case there is only one vendor having technical score of 70 or more, the Bank may, at its sole discretion, also consider the next highest technical score and qualify such vendor. In case, none of the participating vendors qualify on technical criteria and reach or exceed the cut-off score of 70, then the Bank, at its sole discretion, may qualify two bidders on the basis of the top 2 scores. However, the Bank at its discretion may reject the proposal of the Vendor or will not consider vendor below cutoff marks by relaxing as mentioned above, if in the Bank's opinion the Vendor could not present or demonstrate the proposed solution as described in the proposal or in case the responses received from the customer contacts / site visited are negative or the proposed solution does not meet the Bank's functional and technical requirement.

Technical Evaluation Criteria-

ST = Each Technical Proposal will be assigned a Score Technical (ST).

The bidder with highest marks obtained (TM) in technical evaluation will be given a Score Technical (ST) of 100 points. The score technical (ST) of other proposals will be computed as follows:

ST = 100xTS/TM, where TS= marks obtained for Technical Proposal

Based on ST (Score Technical) the bid with highest ST score will be termed as T1. The rest of the bidders shall be ranked in descending order of ST Score value as T2, T3, T4 and so on.

Score will be considered up to two decimal places. Technical qualified bid will be considered once it scores minimum score technical (ST) of 70% and above, and rest will be technically rejected. Commercial will not be opened for technically dis-qualified bid.

2.33. Evaluation of Commercial Bids

Commercial bids submitted by only those bidders, who have qualified in Technical evaluation, will be eligible for further evaluation.

The Commercial Bids of only those Bidders short listed from the Technical Bids by Bank will be opened in the presence of their representatives on a specified date and time to be intimated to the respective Bidders, and the same will be evaluated by Bank.

Bidders will be ranked as per the ascending order of value of their Commercial Bids (As per Section VI Annexure 15 (Commercial Bid Format) as (Least Quoted) LQ1, LQ2, LQ3……and so on, LQ1 being the lowest Financials.

SF = Each commercial Proposal will be assigned a financial score (SF). The lowest GTV (Grand Total Value) (FM) will be given a financial score (SF) of 100 points. The financial scores of other proposals will be computed as follows:

SF = 100 x FM/LQx(1,2,3…), where LQx = Amount of Financial Proposal (GTV)

Based on SF (Score Financial) the bid with highest SF score will be termed as L1. The rest of the bidders shall be ranked in descending order of SF Score value as L2, L3, L4 and so on. Bidders quoting incredibly low or unrealistic high cost of items leading to unrealistic GTV with a view to

subverting the RFP process shall be rejected straight away by Bank and EMD of such vendor will be forfeited. Any bid found to be unsatisfactory in terms of any of the evaluated parameters as mentioned may be rejected and will not be considered for further evaluation.

2.34. Final Bid Evaluation (Techno Commercial Bid):

The Combined Final Score contains 70% weightage for technical evaluation and 30% weightage for commercial evaluation. Therefore, combined and final evaluation will be done on the following basis:
Proposals will finally be ranked according to their combined Techno commercial score (TC) based on the below mentioned formula:
TC = ST*0.7 + SF*0.3
Bidders will be ranked basis their Final Techno Commercial Score (TC) i.e. TC1, TC2, TC3…and so on, TC1 being the highest Combined Final Score.
The shortlisted bidder will be declared after thorough evaluation of commercial bid by Bank. During the evaluation if the Bank finds that the detailed commercial bid is not in order or not complete etc. then Bank will treat his bid as non- viable and same will be rejected, and EMD will be forfeited. In such case the next ranked techno commercial bidder will be considered for further evaluation and so on till a bidder is selected.
If any bidder withdraws his bid, at any stage after the submission of the bid, till the final evaluation or declaration of the final selected bidder, it will be declared a defaulting bidder and EMD of such defaulting bidder will be forfeited and THE NAINITAL BANK LTD. reserves right to blacklist such bidders for next three years from participating in any THE NAINITAL BANK LTD. tender/RFP.
In such situation the RFP process will be continued with the remaining bidders as per their ranking.
If the bidder backs out after being declared as selected bidder, it will be declared a defaulting bidder and EMD of such defaulting bidder will be forfeited and THE NAINITAL BANK LTD. reserves right to blacklist such organization for next three years from participating in any THE NAINITAL BANK LTD. tender/RFP. In such case the detailed commercial bid of next ranked techno commercial bidder will be evaluated,

a) If the detailed commercial bid is found in order, complete and its GTV is less than the withdrawing bidder, then this bidder will be declared as selected bidder and will provide services at its own quoted rates.
b) In case the GTV of next ranked techno commercial bidder is higher than the withdrawing bidder, then it should match the detailed commercial bid offered by withdrawing bidder in *to.*
c) If next ranked techno commercial bidder also backs out, then the Bank will complete the RFP process by following the aforesaid process again for other remaining techno- commercial ranked bidders.

Please note that if, after various rounds of evaluation to shortlist a Bidder in place of defaulting bidder, the Bank does not find any suitable bidder amongst remaining eligible bidders, then the Bank shall be at its liberty to reject or accept the bid of the next ranked techno commercial bidder.

2.35. Bank's right to vary scope of contract at the time of award:

The Bank may at any time, by a written order given to the Bidder, make changes to the scope of the Contract as specified.

If any such change causes an increase or decrease in the cost of, or the time required for the Bidder's performance of any part of the work under the Contract, whether changed or not changed by the order, an equitable adjustment shall be made in the Contract Value or time schedule, or both, as decided by the bank and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause must be asserted within thirty (30) days from the date of the Bidder's receipt of the Bank's changed order.

2.36. Bank's right to accept any Bid and to reject any or all bids:

The Bank reserves the right to accept any bid, and to annul the RFP/Tender process and reject all bids at any time prior to award of Contract, without thereby 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.

2.37. Notification of award:

Prior to the expiration of the period of bid validity (180 days from last date of bid submission), the Bank will notify the successful Bidder in writing that its bid has been accepted.
The notification of award will constitute the formation of the Agreement/Contract, requiring the successful Bidder to furnish Bank Guarantee, favouring The Nainital Bank Ltd. of 10% of the purchase order Value for ensuring contract performance. Thereafter the Bank will notify each unsuccessful Bidder and will return/release its EMD.

2.38. Award of Contract:

There will be only one vendor.
At the same time as the Bank notifies the successful Bidder that its bid has been accepted, the Bank will send the Bidder the Pro forma of Contract /Agreement.
Within 15 days of receipt of the Pro forma of Contract/Agreement, the successful Bidder shall sign and date the Contract/Agreement and return it to the Bank along with the Bank Guarantee, favouring The Nainital Bank Ltd. for contract performance as security deposit.

The term of this Contract will commence from the date of signing of contract/agreement and will be valid for a period of five (5) years which will be computed from the date of Go-Live of proposed solution. (Apart from above said 5 years' term, both Bank and Bidder shall also be governed by the terms of the said agreement for the term of preparation period i.e. the period between date of signing of agreement till date of go-live of solution). The contract is extendable further for three (3) years solely at the discretion of the Bank.
Keeping in view the commitment, The Nainital Bank Ltd. reserves the right to ask the Bidder to add new features/ process or modify the existing services to take care the service delivery as and when required.

Bidders has to agree for honouring all RFP conditions and adherence to all aspects of fair trade practices in executing the purchase orders placed by THE NAINITAL BANK LTD.

If the name of the system/service/process/solution is changed for describing substantially the same in a renamed form; then all techno-fiscal benefits agreed with respect to the service, shall be passed on to

THE NAINITAL BANK LTD. and the obligations with THE NAINITAL BANK LTD. taken by the vendor(s) with respect to the service with the old name shall be passed on along with the service so renamed.

The above Security Deposit will be in the form of Bank Guarantee (BG) of any Scheduled Commercial Bank other than the Nainital Bank Limited. Security Deposit should be valid for the entire contract period of 60 months and renewed for extended period, if required, and thereafter on satisfactory performance and completion of contract, the Security Deposit shall be refunded to the vendor without any interest.

2.39. Termination of contract:

1. The Bank shall serve the 30 days' notice of termination to the Shortlisted bidder before terminating the contract of the selected.
2. The Bank will be entitled to terminate the contract, without any cost to the Bank and recover expenditure incurred by the Bank, on the happening of any one or more of the following:
   a. The selected bidder commits a breach of any of the terms and conditions of the bid.
   b. The selected bidder goes into liquidation voluntarily or otherwise or appointment of receiver or manager of any of the successful bidder's assets or insolvency of the successful bidder.
   c. Distress, execution or other legal processes being levied on or upon any of the successful bidder's goods and/ or assets.
   d. If the successful bidder assigns or attempts to assign his interest or any part thereof of the project assigned.
   e. An attachment is levied or continues to be levied for a period of 7 days upon effects of the Agreement.
   f. The progress regarding the execution of the order accepted by the successful bidder is found to be unsatisfactory or delay in execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving 30 days' notice for the same. In this event, the successful bidder is bound to make good the additional expenditure, which the Bank may have to incur in executing the balance contract. This clause is applicable, if for any reason the contract is cancelled/terminated.
   g. Non-satisfactory performance of the successful bidder during implementation and operation.
   h. An act or omission by the successful Bidder, its employees or its agents in the performance of the services provided in the contract and this RFP including delay in performance of the services beyond the specified period or any other reason which in the judgment of the Bank does warrants termination of contract
   i. Failure to perform services to the satisfaction of Bank.
   j. Material discrepancies in the Services noted by the Bank. The Bank reserves the right to procure the same or similar service from the alternate sources at the risk, cost and responsibility of the Successful bidder.
   k. Successful bidder is found to be indulging in frauds.

l. The Bank suffers a reputation loss on account of any activity of empaneled vendor or penalty is levied by regulatory authority.

m. In the event of sub contract or assignment contrary to the terms of agreement

THE NAINITAL BANK LTD. may, at any time, terminate the contract by giving written notice of -30- days to the vendor(s) without any compensation, if the vendor(s) becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to THE NAINITAL BANK LTD. If at any point during the contract, if the vendor(s) fails to, deliver as per the RFP terms and conditions or any other reason amounting to disruption in service, the Termination and Exit Management clause to be incorporated in contract, will be invoked. In case of any takeover/merger/acquisition/transfer of ownership of bidder, the responsibility for smooth transition to the new entity lies with the Bidder at no extra cost. Moreover, Bank will be informed in advance through written notice of likely event of any takeover/merger/acquisition/transfer of ownership of Bidder. If the contract is terminated by the Bank, the Bank shall also be entitled to get back the infrastructure and hardware, if any, provided by the Bank. Termination of contact by the Bank may also be accompanied by a de-facto blacklisting of the successful bidder.

2.40. Conflict of Interest:

The Bank requires that bidder shall provide professional, objective, and impartial advice and at all times hold the Bank's interest paramount, strictly avoid conflicts with other Assignment(s)/ Job(s) or their own corporate interests and act without any expectations/ consideration for award of any future assignment(s) from the Bank. Bidder has an obligation to disclose any situation of actual or potential conflict in assignment/job, activities and relationships that impacts their capacity to serve the best interest of the Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if the Bank comes to know about any such situation at any time, it may lead to the disqualification of the Bidder during bidding process or the termination of its Contract during execution of assignment.

2.41. Placing of Purchase Orders

Purchase order will be placed on the vendor in hardcopy format for procurement of proposed solution / Service.

Objection, if any, to the Purchase Order must be reported to the Bank by the vendor within five (5) working days counted from the date of receipt of Purchase Order for modifications, otherwise it is assumed that the vendor has accepted the Purchase Order.

If the vendor is not able to supply/deploy/operationalize the ordered System/Service completely within the specified period, the penalty clause will be invoked.

The decision of THE NAINITAL BANK LTD. shall be final and binding on all the vendors to this document. THE NAINITAL BANK LTD. reserves the right to accept or reject an offer without assigning any reason whatsoever.

2.42. Confidentiality of the Document

The RFP Document to be submitted by bidder is confidential and the Bidder shall ensure that anything contained in RFP Document shall not be disclosed in any manner, whatsoever. The document contains information confidential and proprietary to the Bank. Additionally, the bidder will be exposed by virtue of the contracted activities to internal business information of the Bank and Associates. The bidder shall ensure that its own employees or the employees/firm(s) engaged/hired by him shall maintain full confidentiality of the entire information. Disclosure, reproduction, transmission of this RFP, any amendment to the RFP, any specifications, plan, drawing, pattern, sample data or any part of the aforementioned information to parties not directly involved in providing the services requested could result in disqualification of bidder, premature termination of the contract or legal action against the bidder for breach of trust.

No media release/public announcement or any other reference to the RFP or any programme thereunder shall be made without written consent of the Bank. Reproduction of the RFP or any other written document without written consent of the Bank by Photographic, electronic or other means is strictly prohibited. The Successful bidder will be required to sign a Confidentiality and non-disclosure agreement with Bank.

2.43. RFP Related Condition

The Bidder should confirm unconditional acceptance of full responsibility of completion of job and for executing the 'Scope of Work' of this RFP on being allotted the project by the Bank. This confirmation should be submitted as part of the Technical Bid. The Bidder shall also be the sole point of contact for all purposes of the Contract.

The Bidder should not be involved in any major litigation/arbitration that may have an impact of affecting or compromising the delivery of services as required under this contract. If at any stage of RFP process or during the currency of the Contract, any suppression / falsification of such information is brought to the knowledge of the Bank, the Bank shall have the right to reject the bid or terminate the contract, as the case may be, without any compensation to the Bidder and claim damages before the court of law, resulting from such rejection/termination as the case may be.

2.44. Prevention of Corrupt and fraudulent practices:

It is required that every participating bidder is required to sign an integrity pact as per the section VI Annexure-17 of this RFP.

1. Every Bidders / Suppliers / Contractors are expected to observe the highest standard of ethics during the procurement and execution of such contracts in pursuance of the policy:
2. "Corrupt Practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution AND
3. "Fraudulent Practice" means a misrepresentation of facts in order to influence a procurement process or the execution of 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.

4. The Bank reserves the right to reject a proposal for award if it determines that the Bidder recommended for award has engaged in corrupt or fraudulent practices in competing for the contract in question.
5. The Bank reserves the right to declare a firm ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the firm has engaged in corrupt or fraudulent practices in competing for or in executing the contract

2.45. Rejection Criteria

Besides other conditions and terms highlighted in the RFP Document, bids may be rejected under following circumstances:

2.45.1 General Rejection Criteria

- Bids submitted without or improper EMD and/or Application Money.
- Bids received through Telex /Telegraphic / Fax/E-Mail will not be considered for evaluation.
- Incomplete Bids, including non-submission or non-furnishing of requisite documents/ Conditional Bids / Bids not conforming to the terms and conditions stipulated in this RFP are liable for rejection by the Bank.
- Bids which do not confirm unconditional validity of the bid as prescribed in the RFP.
- If the information provided by the Bidder is found to be incorrect/ misleading at any stage / time during the RFP Process.
- Any effort on the part of a Bidder to influence the Bank's bid evaluation, bid comparison or contract award decisions.
- Bids received by the Bank after the last date and schedule time for receipt of bids as prescribed by the Bank.
- Bids without letter of authorization and without any other document consisting of adequate proof of the ability of the signatory to bind the Bidder.
- Bid without integrity pact

2.45.2 Technical Rejection Criteria

- Technical Bid containing commercial details.
- Revelation of Prices in any form or by any reason before opening the Commercial Bid.
- Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the RFP Document in every respect.
- Bidders not quoting for the complete scope of Work as indicated in the RFP Documents, corrigendum/addendum (if any) and any subsequent information given to the Bidder.
- Bidders not complying with the material technical requirement by way of functionality, specifications and General Terms and conditions as stated in the RFP Documents.
- The Bidder not confirming unconditional acceptance of full responsibility of providing services.
- If the bid does not confirm to the timelines indicated in the bid.
- Bidder not scoring minimum marks as mentioned in RFP

2.45.3 Commercial Rejection Criteria

- Incomplete Financial Bid.
- Financial Bids that do not conform to the RFP's Financial bid format.
- Total price quoted by the Bidder does not clarify regarding all statutory taxes and levies applicable.
- If there is an arithmetic discrepancy in the commercial bid calculations the Bank shall rectify the same at its discretion. If the Bidder does not accept the correction of the errors, its bid may be rejected

3. Section III: Detailed Scope of Work

Bank intends to implement Fraud Risk Management System. Detailed scope is mentioned below in section VI Annexure-11

Note: - Scope of supply also includes components, materials, accessories required to render the system offered complete in all respects even though every individual item may not have been specifically mentioned in the RFP. Bank will award the contract to the successful vendor who should deliver the solution with the detailed scope mentioned in the Technical Requirement in Annexure-11.

3.1. Upgrades and Updates

- The bidder shall be required to provide all future updates and upgrades for the proposed Solution/Application free of cost during contract period. If, however, the upgrades and/or updates are not available or the solution(software) is declared End of Life/End of Support, Bidder has to upgrade the solution to an equivalent or higher solution without any additional cost to the Bank.
- The bidder should inform to the Bank if any new version, service pack, upgrade of the proposed solution is released, within seven (7) days of such release and deploy the upgraded solution and endpoints within 15 days of such release without any cost to the Bank covering all patches, man-day efforts at the respective locations (DC & DR) of the Bank during the period of the contract.
- During the period of the contract, all upgrades, updates or requirements in software, implementation of upgrades, patches, version changes etc., due to whatsoever reason including but not limited to EOL(End-of-Life) or EOS(End-of-Support), shall be done by the bidder within stipulated time but not later than one month without any additional cost to the Bank. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during the period of contract, the bidder shall upgrade with equivalent or higher specifications as stated above, at no additional cost to the Bank.

4. Section IV – General Conditions of Contract and Service Levels Agreement

4.1 Quality

Material/solution not confirming to given specifications will be rejected & it will be replaced by the vendor, free of cost. The material/solution must be as per the detailed specifications listed out

in RFP document and shall be as per standard engineering practice, relevant IS/ Imitational code of practice, and shall be as per the Specifications as mentioned in RFP Document.

4.2 Statutory Laws

Vendor shall abide by all applicable rules and regulations regarding taxes, duties, labour etc., which are in force and from time to time enforced by the Government of India, also registration, labour laws, payments, ESIC, PF, insurance etc. Vendor shall coordinate for all these matters with concerned authorities directly.

4.3 Confidential Information

All information exchanged between the parties will be confidential. If the implementation project requires disclosure of, or receipt of, confidential information, such disclosure or receipt will be made with mutual agreement and may be with a separately executed MoU / Non-Disclosure agreement with Vendor by the Bank.

4.4 Extra Deviated Items

Any extra item like variation in quantity, deviated item should be executed only after getting the appropriate approvals with written confirmation, from the bank. At the time of submitting the invoice, all the documentary evidence of appropriate approvals for Extra / deviated Items / Variation in Quantities should be attached. Payments will not be made without scrutiny of aforesaid approvals.

4.5 Force Majure

Bank shall not be responsible for delays or non-performance of any or all obligations, contained in this RFP or agreement thereafter, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, Plague, epidemics or pandemics, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of the bank, which directly, materially and adversely affect the performance of any or all such obligations. However, the bidder shall continue to perform its obligations as contained in this RFP and agreement thereafter.

4.6 Arbitration

The Bank and the Bidder shall make every effort to resolve amicably, by direct negotiation between the respective Designated Officials of the bank and the Bidder, any disagreement or dispute arising between them under or in connection with the RFP and or contract thereafter.
If the designated official of the Bank and the Bidder are unable to resolve the dispute within -30- days from the commencement of such informal negotiations, they shall immediately escalate the dispute to their Senior Authorized Personnel.
If within -30- days from the commencement of such negotiations between the Senior Authorized Personnel designated by the Bidder and Bank, are unable to resolve their dispute amicably, in such case the dispute shall be settled finally by arbitration in, Nainital Uttarakhand, India under and in accordance with the provisions of the Arbitration and Conciliation Act, 1996

or any statutory modification or re-enactment thereof. The right to appoint arbitrator shall lie with the bank only.

a. **Jurisdiction**: The Jurisdiction for all disputes will be in the city of Nainital (Uttarakhand), India.

b. **Safety**: All the safety codes and the preventive measure for this type of work shall be strictly followed. In case of any mishap which causes injury, disability or death of any personnel and staff either on site or offsite during or after the duration of the project due to negligence of the staff of the vendor, shall be sole responsibility of vendor, this shall not be responsibility of Bank in any case. No Claims in this regards shall be paid by Bank.

4.7 Term and Extension of the Contract

The term of this Contract will commence from the date of signing of contract/agreement and will be valid for a period of five (5) years which will be computed from the date of Go-Live of proposed solution. (Apart from above said 5 years' term, both Bank and Bidder shall also be governed by the terms of the said agreement for the term of preparation period i.e. the period between date of signing of agreement till date of go-live of solution.) The contract is extendable further for three (3) years solely at the discretion of the Bank.

The Bank shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Bidder, at least 6 months before the expiration of the Term hereof, whether it will grant the Bidder an extension of the Term. The decision to grant or refuse the extension shall be at the Bank's discretion.

During extended period of three years if deemed appropriate (THE NAINITAL BANK LTD. reserve right to extend the agreement with Bidder), the term and conditions for SLA, penalty and Prices for On-premise services, AMC & Manpower shall remain same as given for 5th Year.

Where the Bank is of the view that no further extension of the term be granted to the Bidder, the Bank shall notify the Bidder of its decision at least 6 (six) months prior to the expiry of the Term. Upon receipt of such notice, the Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the Bank shall either appoint an alternative service provider or create its own infrastructure to operate such Services as are provided under this RFP. In such scenario, the terms and conditions for SLA, penalty and Prices for On-premise services, AMC & Manpower shall remain same as given for 5th Year.

Delivery Timelines:

The Fraud Risk Management System must be implemented as per project scope within a period of 9 months in totality from the date of placing of purchase order by the Bank. However, the solution needs to be rolled out in phases as explained in point 4 Project Timelines Deliverables in Annexure 11.

The implementation should be carried out in three phases:

Phase – I: The vendor must implement the FRM solution and interface with CBS, Debit Card/POS/ E-Commerce, Net Banking, Mobile Banking, SMS and Email gateway in this phase. All other readily available functionalities with CBS data should be available. Phase - I Go-Live is in 3 months from the start of implementation.

Phase – II: All other readily available functionalities in India and interfaces with other systems to cover Asset side frauds, case management, NEFT/RTGS, UPI, IMPS, AePS, Access of System to be available up to identified Regional Centres. Phase - II Go-Live is in 6 months from the start of implementation.

Phase – III: All functionalities covering all types of frauds as per RFP Customizations need to be completed in this phase including Call Centre & IVRS(All Channels), Behavioral Biometric Application Integration, branch transactions* Phase-III Go-Live is in 9 months from the start of implementation.

*Branch Transactions (including monitoring of Internal Accounts, Deposit accounts, Loan accounts, Staff Accounts, New Accounts, Money mules, CTS, NACH, PFMS, Open API etc.) Various external Feeds to be consumed/provided as & when required

In case the deadlines are not met then the vendor will have to pay penalty to Nainital Bank @ 1% of implementation cost inclusive of all taxes, duties, levies etc., per week or part thereof, for late implementation beyond due date of implementation, to a maximum of 5%. If delay exceeds two weeks from due date of implementation, The Nainital Bank Limited reserves the right to cancel the entire order.

Any deliverable has not been implemented or not operational on account of which the implementation is delayed, will be deemed/treated as non-delivery thereby excluding the Bank from all payment obligations under the terms of this contract.

4.8 Exit Management:

In event of termination and/or completion of term of the agreement, the following points will have to be followed before final termination of services, provided the Bank invokes the exit management clause in writing:

- The Vendor shall not immediately delete any data and cease to provide the services to the Bank without the express approval of the Bank.
- The Vendor shall provide the Bank or its nominated agency with an exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the underlying transitioning services.
- Transition of data from existing solution provided by Vendor to the solution provided by new Vendor/bank. Vendor shall be supporting in transition to new vendor/bank and extra scope shall be taken as change request by vendor on chargeable basis on a mutual agreeable rate.
- Migration from the Vendor environment to the new vendor's environment. This activity shall be taken as change request by Vendor on chargeable basis on a mutual agreeable rate.
- In case the vendor terminates the agreement prior to the completion of term OR vendor decides to

provide services from new environment / location during contract period. In such circumstances the Bank shall not be liable to pay any charges towards such transition / migration activities.

- Vendor shall carry out the migration of the data, content and any other asset to the new environment identified by the Bank to enable successful deployment and running of the services desired by the Bank in the new environment. The format/manner in which the data shall be transmitted from the Vendor software solution to the new environment, if possible, shall be identified by the Bank to ease and enhance portability. This activity shall be taken as change request by Vendor on chargeable basis on mutual agreeable rates.
- Vendor shall ensure that all the documentation required by the Bank for smooth transition are kept up to date and all such documentation is handed over to the Bank during regular intervals as well as during the exit management process.
- Vendor shall transfer to the Bank the Physical and logical security processes and tools, including catalogues, badges, keys, documented ownership and access levels for all passwords and instructions for use and operation of security controls developed during the term to support the delivery of the Exit Management Services.
- Vendor shall carry out following key activities including but not limited to, as part of the knowledge transfer:
    a. Preparing documents to explain design and characteristics
    b. Carrying out joint operations of key activities or services
    c. Briefing sessions on processes and documenting processes
    d. Sharing the logs, any other requirement of the Bank etc.
- Vendor shall transfer/ share know-how relating to operation and maintenance of the service, solution, software etc.
- Each Party shall forthwith handover all the Confidential Information, documents, statements, reports, and all other related material of the other Party in its possession to an authorized official of the other Party.
- Bank will not pay anything for the migration of services and data to Vendor's nominated agency/bank.
- Post successful migration of services and data to Bank/Bank's duly nominated agency, Vendor will provide a duly signed certificate that entire Bank's data has been deleted from its systems and it is not in possession of any data and information pertaining to Bank. Without prejudice to any other right under the law and otherwise, please note that the Bank will not provide sign-off to the Vendor without receiving this certificate.
- Post sign-off provided by Bank for successful migration of services and data to its duly nominated agency the Parties shall immediately cease to represent each other or operate under the Agreements and not hold itself in any way as the representative of the other Party and refrain from any action that would or may indicate any other relationship.

4.9 Payment Terms

The Vendor must accept the payment terms proposed by the Bank. The commercial/financial bid submitted by the Vendors must be in conformity with the payment terms proposed by the Bank.

Any deviation from the proposed payment terms would not be accepted. The Bank shall have the right to withhold any payment due to the vendor, in case of delays or defaults on the part of the vendor. Such withholding of payment shall not amount to a default on the part of the Bank. If any of the items / activities as mentioned in the price bid is not taken up by the bank during the course of the assignment, the bank will not pay the professional fees quoted by the vendor in the price bid against such activity / item.

Prices quoted must be firm and shall not be subject to any upward revision on any account whatsoever throughout the period of contract. However, if there is any increase/decrease in taxes/ duties due to any reason whatsoever, after Notification of Award, the same shall be passed on to The Nainital Bank Ltd.

In any circumstances no other additional cost shall be payable by the Bank on account of any software / tools used by the Service Provider for rendering the services as required in the Tender. The bidder should make his own arrangement for providing such software / tools used at his own cost. The responsibility to ensure that only legal, authorized, licensed versions of software / tools provided by the bidder and used by its employees are used for extending the required services, lies solely with the bidder.

The Bank in no way be a part of any litigation arising out of using unauthorized software / tool used by the bidder/service provider.

The payment will be released as follows:

Software Licenses

- 30% of the total cost on delivery of Software Licenses plus GST. The required documents to be provided along with original invoice:
- Original delivery Challans dully stamped and signed by the Bank Official.
- 20% of the total Software Licenses cost after Phase I go-live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.
- 20% of the total Software Licenses cost after Phase II go-live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.
- 30% of the total Software Licenses cost after Phase III go-live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.

Implementation Cost (OTC)

- 30% after Phase I go- live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.

- 20% after Phase II go- live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.
- 20% after Phase III go- live sign off from Bank. Go Live Sign Off in the form of Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative.
- 30% after Go-Live closure signoff from Bank. Go Live Closure Sign Off in the form of Final Acceptance Test should be signed by both Bank's identified Project Manager & vendor representative. Operational Issues will be part of Managed Services and not part of Go-Live Sign Off.

- **AMC / ATS –** Payable quarterly in advance against receipt of satisfactory service report of previous quarter from the Bank's Project / Operation Manager
- **Onsite Support Charges –** Payable quarterly at the end of each quarter against receipt of satisfactory support report of previous quarter from the Bank's Project / Operation Manager

There shall be no escalation in the prices once the prices are fixed and agreed to by the Bank and the vendor. Payment will be release by FRMG(Fraud Risk Management Group) as per above payment terms on submission of mentioned supporting documents.

The Bank will pay invoices within a period of 30 days from the date of receipt of undisputed invoices. Any dispute regarding the invoice will be communicated to the selected vendor within 15 days from the date of receipt of the invoice. After the dispute is resolved, Bank shall make payment within 15 days from the date the dispute stands resolved. General Terms and Conditions

4.10 Security and Audit

- The process and proposed solution deployed by the Successful Bidder will be installed in the Bank's premises/network and has to abide by the information security policy, procedure and guidelines.
- The process & proposed solution will be subject to audit by Bank Appointed Software Audit firm/in house team. All audit points raised by the Audit team should be complied with by the selected Bidder without any extra charge and within the stipulated time frame decided between the Bank and the successful Bidder.
- Successful Bidder may have to get them processes audited by independent auditors if so asked by Bank/ Bank's Auditors; cost of which will be borne by the Bidder.

4.11 Service Level Agreement and Non-Disclosure Agreement

The selected vendor shall execute a) Service Level Agreement (SLA), which must include all the services and terms and conditions of the services to be extended as detailed herein, and as may be prescribed or recommended by the Bank and b) Non-Disclosure Agreement (NDA). The selected vendor shall execute the SLA and NDA within two months from the date of acceptance of letter of appointment or as intimated by the Bank.

5. Section V – Bid Submission Format

5.1 Bidder Profile

To,
The Nainital Bank Ltd,
Head Office, Mallital
Nainital

Sub: Request for proposal (RFP) for

1- Having examined the RFP Documents including all Annexures and Appendices, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, implement and commission ALL the items/activities mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said RFP Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this RFP.

We also submit required information along with documentary evidence in following format:

Sr	Particulars	Details
1.	Name of the Bidder	
2.	Address of the Bidder	
3.	Status of the Company (Public Ltd/ Pvt. Ltd)/Firm/LLP etc.	
4.	Details of Incorporation of the Company/Firm	
5.	Details of Commencement of Business	
6.	GST registration no.	

7.	a. Permanent Account Number (PAN) & b. TAN	
8.	Name & Designation of the authorized contact person to whom all references correspondence shall be made regarding this RFP	
9.	Telephone No. (with STD Code) a) Landline b) Mobile	
10.	E-Mail of the contact person:	
11.	Fax No. (with STD Code)	
12.	Website	
13.	Details of NEFT transaction details (if Application Money and EMD are credited to Bank through electronic mode)	Account Name - APPLICATION MONEY & EMD Account Number - 999421390000001 IFSC Code - NTBL0NAI999 Branch Name - Head Office, Nainital The following details are to be submitted: Sender Account Number: Sender Account Name: UTR Number: IFSC: Bank Name: Date:
14	Details of account wherein the EMD amount is to be returned if the EMD is sent through NEFT	The following details are to be submitted: Account Name – Account Number – IFSC Code – Bank Name - Branch Name -
	Financial Details (as per audited Balance Sheets) (in Cr) only for 2 years included	

	Year	**2022-2023**	**2023 - 2024**
15.	Net Worth		

16.	Turn Over (Total)		
17.	Turn Over (from Indian Operations)		
18.	Turn Over (from data centre operations)		
19.	Profit After Tax (PAT)		
20.	Net Profit		

2. If our Bid is accepted, we undertake to comply with the delivery schedule as mentioned in the RFP Document.
3. We agree to abide by this RFP Offer for 180 days from date of bid opening and our Offer shall remain binding on us and may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".
6. We agree that the Bank is not bound to accept the lowest or any Bid the Bank may receive.
7. We certify that we have provided all the information requested by the bank in the format requested for.

We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Dated this……..by ……..2025
Yours faithfully,
Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

5.2 Declaration for Non-Blacklisting

UNDERTAKING FOR NON- BLACKLISTED

To be provided on letter head of the Bidder's Company

To,
The Chief Operating Officer
Nainital Bank Limited
Head Office
Mallital, Nainital-263001 (Uttarakhand)

Madam/Dear Sir,

Reg.: RFP Reference No: NTB/IT/FRMS/2025/03/023

We M/s _____, a company incorporated under the Companies Act, 1956/2013 with its headquarters at _____, do hereby confirm that we have not been blacklisted/ debarred by the Statutory, Regulatory or Government Authorities or Public Sector Undertakings (PSUs / PSBs) or Private Banks or Financial Institutions in India during last 3 years.

This declaration is being submitted and limited to, in response to the RFP reference mentioned in this document

Thanking You,

Yours faithfully,

Signature of Authorized Signatory
Name of Signatory:
Designation:
Seal of Company

5.3 Undertaking of Information Security

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

To,
The Chief Operating Officer
Nainital Bank Limited
Head Office
Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: RFP Reference No: NTB/IT/FRMS/2025/03/023

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

Dated this……..day of ……2025

Yours faithfully,

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

5.4 Undertaking by the bidder (To be included in Technical & Commercial Bid Envelope)

To be provided on letter head of the Bidder's Company

To,
The Chief Operating Officer
Nainital Bank Limited
Head Office
Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,

Reg.: RFP Reference No: NTB/IT/FRMS/2025/03/023

It is certified that the information furnished here in and as per the document submitted is true and accurate and nothing has been concealed or tampered with. We have gone through all the conditions of bid and are liable to any punitive action for furnishing false information / documents. Dated this ……. day of …… 2025.

Yours faithfully,

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

5.5 Undertaking for Price Validity & Acceptance of all terms & conditions of RFP

To be provided on letter head of the Bidder's Company

To,
The Chief Operating Officer
Nainital Bank Limited
Head Office
Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,
Reg.: RFP Reference No: NTB/IT/FRMS/2025/03/023

We understand that Bank is not bound to accept the lowest or any bid received and Bank may reject all or any bid. We shall keep the price valid for the entire contract period from the date of issuance of the first Work order. If our bid is accepted, we are responsible for the due performance as per the scope of work and terms & conditions as per mentioned in RFP.

Yours faithfully,

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

5.6 Undertaking for No Deviation

To be provided on letter head of the Bidder's Company

To,
The Chief Operating Officer
Nainital Bank Limited
Head Office
Mallital, Nainital-263001 (Uttarakhand)

Madam/Sir,
Reg.: RFP Reference No: NTB/IT/FRMS/2025/03/023

Further to our proposal dated ……, in response to the Request for Proposal (Bank's RFP Ref. No **NTB/IT/FRMS/2025/03/023** hereinafter referred to as "RFP") issued by Bank, we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original RFP documents if any, issued by the Bank. The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #

5.7 Non-Disclosure Confidentiality Agreement

NON DISCLOSURE CONFIDENTIALITY AGREEMENT

(To be submitted by all Bidders for availing the proposed features for Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System (TO BE STAMPED AS AN AGREEMENT AS APPLICABLE TO STATE OF UTTARAKHAND)

This Confidentiality Agreement (the "Agreement") made and entered into on the date signed by the parties:

BETWEEN:

_____ company having its Registered Office _____ (hereinafter referred to as the _____ which expression shall mean and include its Administrator, legal representatives, successors-in-interest, Executors and permitted assigns) and represented herein by its authorized signatory, of the ONE PART;

AND

THE NAINITAL BANK LIMITED, a Scheduled Commercial bank incorporated under the Companies Act, 1956 (now the Companies Act, 2013) having its Registered Office at G.B. Pant Road, Nainital and its Head Office at Seven Oaks Building, Mallital, Nainital (CIN No. U65923UR1922PLC000234) (hereinafter referred to as the "Bank" which expression shall mean and include its Administrator, legal representatives, successors-in-interest, Executors and permitted assigns) and represented herein by its authorized signatory, of the OTHER PART.

_____ and Bank are hereinafter individually referred to as the "Party" and collectively as the "Parties", as the context may require in this Agreement.

WITNESSETH:

WHEREAS,

A. The Bank had floated RFP No. **NTB/IT/FRMS/2025/03/023** dated 21.03.2025 being desirous of getting Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System.
B. In order to avail the services / solution from _____, and the Bank may in the course of discussions, may disclose certain confidential or proprietary information either related to itself or pertaining to its customers in whatever form to the other Party and vice versa; and
C. _____ and Bank desire to safeguard and protect their respective confidential, proprietary or trade secret information.

NOW, THEREFORE, in consideration of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. DEFINITIONS:

1.1. As used herein, the term "Disclosing Party" shall mean: (a) _____, with respect to all Confidential Information disclosed by _____ to Bank hereunder; or (b) Bank, with respect to all Confidential Information disclosed by Bank to _____ hereunder.

1.2. As used herein, the term "Receiving Party" shall mean: (a) Bank, with respect to all Confidential Information disclosed by _____ to Bank; or (b) _____, with respect to all Confidential Information disclosed by Bank to _____ hereunder.

1.3. As used herein, the term "Confidential Information" shall mean all confidential or proprietary information of the Disclosing Party or its subsidiaries or affiliates, including (whether or not reduced to writing), which is disclosed or made available by the Disclosing Party to the Receiving Party and/or its Representatives and that is expressed and/or marked at the time of disclosure to be of a confidential nature, or which under the circumstances surrounding the disclosure ought to be treated as confidential. Confidential Information includes, but is not limited to (i) non-public information relating to the Disclosing Party's technology, products, services, processes, data, customers information interalia phone number, e-mail address, business plans and methods, promotional and marketing activities, finances and other business affairs, (ii) third-party information that the Disclosing Party is obligated to keep confidential, and (iii) the nature, content and existence of a Relationship, discussions or negotiations between the parties.

Notwithstanding the foregoing, Confidential Information shall not include information which:

a) was in the public domain on the date hereof or comes into the public domain other than through the fault or negligence of the Receiving Party;
b) was lawfully obtained by the Receiving Party without restrictions from a third party who has the right to disclose it;
c) was known to the Receiving Party at the time of disclosure as shown by its written records in existence at the time of disclosure;
d) was independently developed by the Receiving Party without making use of any Confidential Information nor other information that the Disclosing Party disclosed in confidence to any third party; or
e) was excluded from the scope of the confidentiality obligation hereunder with the Disclosing Party's written consent; or
f) is disclosed to the Receiving Party from any third party, except where the Receiving Party knows, or reasonably should know, that such disclosure constitutes a wrongful or tortious act.

2. NON-DISCLOSURE:

2.1 In consideration of the Disclosing Party's disclosure of Confidential Information to the Receiving Party, the Receiving Party agrees that it shall:

(i) treat all Confidential Information as strictly confidential and shall not disclose the such information to any person or entity, whatsoever, unless otherwise provided for in this agreement;

(ii) not use any Confidential Information except for the Evaluation in connection with the Relationship;
(iii) protect all Confidential Information, whether in storage or in use, with the same degree of care as the Receiving Party uses to protect its own Confidential Information against public disclosure, but in no case with less than reasonable care;
(iv) inform the Disclosing Party immediately on becoming aware, or suspecting that an unauthorised person has become aware of the Confidential Information; and
(v) be entitled to disclose the Confidential Information to such directors, officers, employees, agents, contractors and advisors of the Receiving Party who need to know such Confidential Information for the Evaluation (collectively the "Representatives"). "Provided always that the Receiving Party shall, prior to disclosure, inform the Representatives of the confidential nature of such Confidential Information and impose on such Representatives the confidentiality obligations substantially equal to, but not less restrictive than, those set forth herein. In any event, the Receiving Party shall be responsible for any breach of the terms of this Agreement by any of its Representatives and shall take all appropriate measures to restrain its Representatives from prohibited or unauthorised disclosure or use of the Confidential Information.

2.2 If Receiving Party is required to disclose the Confidential Information pursuant to law, regulation, the order of any court or governmental or regulatory agency or the rules of any applicable stock exchange, the Receiving Party shall, to the extent permitted by law or regulation, (i) immediately notify the Disclosing Party of any such requirement and afford such Disclosing Party the opportunity to seek a protective order relating to any such disclosure; (ii) only furnish the portion of the Confidential Information that is required to disclose; and (iii) exercise all reasonable efforts to obtain reliable assurances that confidential treatment will be accorded with respect to the Confidential Information disclosed. The Receiving Party shall, to the extent reasonable and practicable, co-operate with the Disclosing Party if the Disclosing Party decides to bring any legal or other proceedings to challenge the validity of the requirement to disclose the Confidential Information (at the Disclosing Party's cost and expense). If the Receiving Party is unable to inform the Disclosing Party before any Confidential Information is disclosed, the Receiving Party shall inform the Disclosing Party immediately after the disclosure of the full circumstances of the disclosure and the information that has been disclosed.

2.3 Except upon mutual written agreement, or as may be required by law, regulation, the order of any court or governmental or regulatory agency or the rules of any applicable stock exchange, neither Party shall in any way or in any form disclose the fact that this Agreement has been signed by the Parties, the fact that discussions or negotiations relating to the Evaluation are taking place or have taken place, and any of the terms, conditions or other facts relating to the Evaluation, including the status thereof, or make any public announcement pertaining to the foregoing including any such actual or possible discussions or negotiations.

3. RETURN OF CONFIDENTIAL INFORMATION:

Upon request of the Disclosing Party made at any time during the term of this Agreement or within thirty (30) days after its termination, the Receiving Party shall, at the Disclosing Party's sole option, promptly return to the Disclosing Party or destroy all items of Confidential Information (including without limitation all summaries, copies and excerpts of Confidential Information thereof) of the Disclosing Party. The receiving party shall furnish a certificate to the disclosing party whereby certifying that the all confidential information has been returned to the Disclosing Party or has been destroyed and nothing can be retrieved by it in any manner whatsoever.

OWNERSHIP:

All rights, title and interest in and to the Confidential Information disclosed by the Disclosing Party shall remain the exclusive property of the Disclosing Party. The Parties acknowledge and agree: (i) that this Agreement shall not be construed as a transfer or sale by the Disclosing Party of any rights whatsoever, by license or otherwise, in or to any of its Confidential Information and; (ii) that no licenses or rights under any patent, copyright, trademark, trade secret or intellectual property rights shall be made, granted or implied by this Agreement. Any and all Confidential Information disclosed hereunder are disclosed under the sole discretion of the Disclosing Party, to the extent that the Disclosing Party deems it necessary in connection with the Evaluation. Nothing contained herein shall be construed as bearing an obligation on either Party to disclose any Confidential Information. In the event that the Receiving Party should request or agree to receive Confidential Information which the Disclosing Party has received from a third party, and the Disclosing Party is bound by the terms of a confidentiality agreement with such third party ("Confidentiality Agreement"), then the Receiving Party shall, subject to its receiving a copy of the relevant Confidentiality Agreement from the Disclosing Party, agree to act in accordance with the terms and conditions of the Confidentiality Agreement set forth by the third party.

5. INJUNCTIVE RELIEF:

Both Parties acknowledge that the extent of damages in an event of the breach of any provision of this Agreement would be difficult or impossible to ascertain, and that there may be no adequate remedy available at law in the event of any such breach. Therefore, each Party agrees that in the event it breaches any provision of this Agreement, the other Party will be entitled to specific performance and injunctive or other equitable relief, in addition to any other relief to which it may be entitled to at law or in equity. Any such relief shall be in addition to and not in lieu of any appropriate relief in the way of monetary damages.

6. TERM:

a. The term of this Agreement shall, unless otherwise agreed between the Parties in writing, shall commence from _____i.e. from the date of execution of this agreement.

b. **Survival**: All obligations created by this Agreement shall survive change or termination of the parties' business relationship for a period of five years from the date of the disclosure of the Confidential Information or the change in/termination of the business relationship of the parties whichever is later.

7. INDEMNITY:

The Parties agree to indemnify and keep indemnified each other against all loss and damage, which the Disclosing Party may suffer as a result of any breach of this Agreement by the Receiving Party, provided always that the Disclosing Party shall forthwith give written notice to the Receiving Party of the above loss and damage and satisfactory documentary evidence of such actual loss and damage.

8. GENERAL:

8.1 The Parties agree and acknowledge that the Confidential Information constitutes valuable proprietary information and that the provisions of this Agreement are fair and reasonable to protect the interests of the Disclosing Party.

8.2 This Agreement shall be governed by and construed in accordance with the laws of India without reference to the principles of conflict of laws. All disputes arising out of or in connection with this Agreement shall be finally settled by panel of three arbitrators, wherein one each arbitrator shall be appointed by each party and such appointed arbitrators shall nominate a third arbitrator. The place of arbitration shall be at Nainital. The arbitration shall be conducted in the English language. The Parties agree that the decision of the arbitrator(s) shall be final and binding and that the Parties shall waive any right of appeal to the courts having jurisdiction in relation to such arbitration. Provided that nothing in this Agreement shall prevent either party from seeking injunctive or similar preliminary or provisional relief from court of competent jurisdiction in accordance with the applicable law.

8.3 In the event any provision of this Agreement shall for any reason be held to be invalid, illegal or unenforceable in any respect, the remaining provisions of this Agreement shall remain in full force and effect to the maximum extent possible.

8.4 This Agreement constitutes the entire agreement between the Parties relating to the subject matter hereof and may not be amended or in any manner modified except by a written instrument signed by authorized representatives of both Parties. All prior or contemporaneous agreements or understandings between both Parties relating to the subject matter hereof, whether oral or written are superseded and cancelled by this Agreement.

8.5 This Agreement is made for the benefit of the Parties to it and their respective successors and permitted assigns and is not intended to benefit or be enforceable by anyone else. A person who is not a party to this Agreement shall have no right to enforce any of the terms of this Agreement. For the avoidance of doubt, the Parties may terminate, rescind or vary this Agreement without the consent of any person who is not a party to this Agreement.

8.6 No provision of this Agreement shall be deemed waived by either Party unless such waiver is reduced to writing and is signed by the Party against whom such waiver is sought to be enforced. Any waiver of any breach of any provision of this Agreement shall not be construed as a waiver of any continuing or succeeding breach of such provision, a waiver of the provision itself or a waiver of any right under this Agreement.

8.7 Neither Party shall transfer or assign its rights or obligations under this Agreement in whole or in part without the prior written consent of the other Party.

8.8 The Disclosing Party does not make any representation or warranty (express or implied) herein as to the accuracy, fairness or completeness of the Confidential Information or as to whether it is up-to-date. The Receiving Party will use the disclosed Confidential Information on an “As Is” “Where Is” basis and

the Disclosing Party shall not have any liability or responsibility for errors or omissions in, or any decisions made by the Receiving Party in reliance on, any Confidential Information disclosed under this Agreement.

8.9 Nothing contained in this Agreement or in any discussions held or disclosures made pursuant to this Agreement shall (i) be interpreted or relied upon by either Party as a commitment or intent to purchase or sell any products or services or to engage in any business relationship, contract or future dealing with the other Party, (ii) limit either Party's right to provide or offer to provide products or services similar to those which the other Party may offer, so long as said Party does not violate the obligations under this Agreement, or (iii) prevent either Party from entering into similar discussions with unrelated third parties so long as such discussions do not violate the obligations under this Agreement.

8.10 This Agreement may be executed in one or more counterparts, which together shall constitute one and the same agreement, and any Party may enter into this Agreement by executing a counterpart.

8.11 All notices hereunder will be given in writing, will refer to this Agreement and will be personally delivered or sent by overnight courier, electronic mail, or registered or certified mail (return receipt requested) to the address set forth below:

For _____:	For Bank:

8.12 Each Party warrants that the executants of this Agreement have full authority to execute this Agreement and upon execution of this it shall be binding and enforceable upon the Party. The parties have executed this Agreement as of the Effective Date.

IN WITNESS WHEREOF, the Parties, by their duly authorized representatives, have executed this Agreement as of the date first set forth above.

Parties	For and behalf of _____	For and on behalf of The Nainital Bank Limited
Signature		
Signatory Name		
Title		
Witness	In the presence of	In the presence of
Signature		
Name		
Designation		
Date		

6. Section VI – Annexure

Annexure 01 – Eligibility Bid - Table of Contents

Eligibility Bid to contain the following

Section #	Section Heading	Pro forma Given
1	Index	**Bidder to provide**
2	Covering letter certifying eligibility criteria compliance	**Bidder to provide**
3	Eligibility criteria compliance with vendor comments	**Annexure 02**
4	Credential letters / Purchase orders / Supporting documents	**Bidder to provide**
5	Application Money Demand Draft/NEFT Details	**Bidder to provide**
6	Bid Security Letter	**Annexure 03**
7	Bid Security (Earnest Money Deposit) Or Bid Security Form (Earnest Money Deposit in the form of Bank Guarantee)/NEFT Details	**Bidder to provide DD or Annexure 04**
8	Undertaking Letter	**Annexure 05**
9	Conformity with Hard Copy	**Annexure 07**
10	Conformity Letter	**Annexure 08**
11	Letter of Undertaking from OSD / OEM	**Annexure 09**
12	Undertaking of Information Security	**Annexure 10**
13	Copy of the tender document along with the addendum duly sealed and signed on all the pages of the document.	**Bidder to provide**
14	Pen Drive containing soft copy of the Annexures and the scanned copies of supporting documents.	**Bidder to provide**
15	Integrity Pact	**Annexure 16**
16	Letter of authorization from the company authorizing the person to sign the tender response and related documents.	**Bidder to provide**

17	Declaration for Non-Blacklisting	**Section V Point 5.2**
18	Undertaking of Information Security	**Section V Point 5.3**
19	Undertaking for No Deviation	**Section V Point 5.6**
20	Executive Summary	**Annexure 17**

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

Annexure 02 - Eligibility Criteria

Eligibility criteria compliance with vendor comments

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
A	**General**		
1	Bidder should be Government Organization / PSU / PSE / partnership firm under Partnership Act / LLP /private or public limited company in India at least for last 3 years as on date of bid.	Documentary Proof to be attached (Certificate of Incorporation). Submit copy of PAN Card, GST Registration.	
2	Bidder must not be blacklisted / debarred by any Statutory, Regulatory or Government Authorities or Public Sector Undertakings / Banks (PSUs / PSBs) or Private Banks or Financial Institutions since last 3 FY years and till date.	Letter of confirmation (self-certified letter as per the format given in pt. 5.2 signed by authorized official of the bidder)	
3	Bidder/OSD must be in business of providing Fraud Risk Management at least for last 2 years.	Documentary Proof to be attached	
4	Bidder to provide an undertaking on his letter head that all the functional and technical requirements highlighted as part of Technical Scope are covered in totality in the proposal submitted.	Letter of confirmation from Bidder	
5	The Bidder to 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 has not participated in the bid process.	Letter of confirmation from Bidder.	
6	Bidder/OSD should have direct employees of at least 50 in their payroll.	Self-declaration in the bidder letterhead duly signed by the authorized person should be submitted	

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
B	**Financial**		
1	Bidder should have minimum annual turnover (from Indian operation) of Rs 10 crores each during the last two financial years that is 2022 – 23 and 2023 - 24 as per audited financial statements.	Audited financial statement of last two financial years	
2	Must be net profit making entity (from Indian operations only) for each year in the last two financial years that is financial years – 2022 – 23 and 2023 - 24.	Audited Financial statements for the financial years 2022 – 23 and 2023 - 24. Certified letter from the Chartered Accountant. The CA certificate in this regard should be without any riders or qualification	
C	**Technical**		
1	If OSD is bidding directly they cannot submit another bid with any Bidder.	Letter of confirmation from OSD need to be submitted.	
2	The Bidder should be an OSD or authorized partner of OSD for supply of licenses and solution implementation and maintenance support under warranty / AMC / ATS for the solution.	Letter of confirmation from OSD need to be submitted.	
3	If Bidder (partner of Original Solution Developer (OSD) is not able to fulfil its obligation to support the solution during the contract period, OSD will have to ensure support as per contract. An undertaking from the OSD to this effect must be submitted	Letter of confirmation from OSD need to be submitted.	
4	One Bidder can bid only with one OSD and similarly one OSD can bid with only one Bidder	Letter of confirmation from OSD need to be submitted.	

S. No	Eligibility Criteria	Supporting Required	Complied (Yes/No)
D	**Experience & Support Infrastructure**		
1	Bidder/OSD should have implemented FRMS/transaction monitoring in at least two Banks / Financial Institutions in India having customer base of 10 Lacs or above and should have experience of integration in their solution with following channel : Core Banking, Mobile Banking, Internet Banking, UPI.	Documentary Proof of order / contract copy / customer credentials.	
2	Bidder/OSD should have direct support offices in Delhi NCR then an undertaking to be provided by the Bidder stating that direct support would be provided by the bidder at Delhi NCR whenever desired by the Bank	Letter of confirmation from the Bidder	
3	The bidder/OSD should be a valid ISO 9000/9001 or ISO/IEC 27001 certification holder company for the IT related activities.	Copy of the ISO 9000/9001 or ISO/IEC 27001 certificate should be submitted along with the Technical bid	
4	Labour Law Compliances	Certificate is to be provided by the chartered accountant /statutory auditor/ Self-undertaking as per Annexure 13	
5	Bidder/OSD should have all necessary licenses, permissions, no objections, 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 to be submitted.	

All dates if not specified to be applicable from the date of the RFP.

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

Annexure 03 - Bid Security Letter

1. WHEREAS, …… (hereinafter referred to as “Vendor”) has submitted its proposal and response dated (hereinafter referred to as “Bid”) for the Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System of all the requirements described in the Request for Proposal No. ……. along with its amendments/annexures and other ancillary documents (hereinafter referred to as “RFP”) as issued by The Nainital Bank Limited.

2. We …… …… …. having our registered office at ……. (hereinafter called the 'VENDOR') are offering security deposit of Rs. /- (Rupees only) vide [demand draft/ pay order / issued by a Scheduled / Commercial bank] bearing No. dated [drawn on/ issued by] (hereinafter referred to as “Bid Security”) favouring ‘The Nainital Bank Limited for consideration of the Bid of the above mentioned Vendor.

3. The Vendor specifically acknowledges and agrees that the Vendor has furnished his Bid on the understanding and condition that, if the Vendor:
   a) Withdraws its Bid during the period of Bid validity specified by the Vendor on the Tender Documents or
   b) Having been notified of the acceptance of its Bid by The Nainital Bank Limited during the period of validity: -
      i. Fails or refuses to execute the contract form if required; or
      ii. Fails or refuses to furnish the Security Deposit / Performance Guarantee, in accordance with the instruction to Vendors.

   The Nainital Bank Limited has the right to forfeit the entire Bid Security amount merely on the occurrence of one or more of the foregoing events without demur or a written demand or notice to the Vendor. The Bid Security shall be returned to unsuccessful Vendors within thirty (30) days from the date of the award of contract to a successful Vendor. The Bid Security shall be returned to the successful Vendor upon furnishing of Performance Security in accordance with the instructions of the Vendor.

4 The Vendor undertakes that it will not cancel the Bid Security referred to above till the Vendor is returned the Bid Security from The Nainital Bank Limited in accordance with the foregoing conditions.

5 The Vendor represents and warrants that the Vendor has obtained all necessary approvals, permissions and consents and has full power and authority to issue this Bid Security and perform its obligations hereunder, and the Vendor has taken all corporate, legal and other actions necessary or advisable to authorize the execution, delivery and performance of this Bid Security. The absence or deficiency of authority or power on

the part of the Vendor to issue this Bid Security or any irregularity in exercise of such powers shall not affect the liability of the Vendor under this Bid Security.

Dated this.....day of..... Place:

Date: Seal and signature of the Vendor

Annexure 04 - Bid Security Form

(FORMAT OF BANK GUARANTEE (BG) IN LIEU OF EARNEST MONEY DEPOSIT)

THIS DEED OF GUARANTEE made at …….. this ……..day of …….. between Bank of …… a banking company having its office at …… hereinafter referred to as 'the Bank' of the One Part and The Nainital bank Limited constituted under the Companies Act, 1956 having its Head Office at Seven Oaks Building Mallital Nainital, hereinafter called the Beneficiary, of the other Part.

Whereas the Beneficiary had invited tenders for _____, vide tender No: _____ dated: _____

One of the terms of the tender is that bidder are required to give a Demand Draft drawn in favour of beneficiary and payable at_____, (valid for _____ days from_____) for Rs _____/- (Rs. XXXXXXX only) as Earnest Money Deposit (EMD) along with their offer. The Beneficiary may accept Bank Guarantee in lieu of EMD for an equivalent amount issued by any Public Sector Bank, valid for 6 months from the date of issue.

M/s <Bidder Name>. hereinafter referred to as the said 'Bidder' have given their offer to _____ the said bidder are required to deposit the said amount of earnest money (or security deposit) or to furnish bank guarantee.

At the request of the said M/s.<Bidder Name>. Ltd. the Bank has agreed to furnish guarantee for payment of the said amount of earnest money (or security deposit) in the manner hereinafter appearing:

NOW THIS DEED WITNESSETH that pursuant to the said tender and in consideration of the promises the Bank doth hereby guarantee to and covenant with the Beneficiary that the Bank shall, whenever called upon by the Beneficiary in writing and without demur and notwithstanding any objection raised by the said bidder pay to the Beneficiary the said amount of Rs. XXXXX/- (Rs. XXXXXXX only) payable by the said bidder under the said Contract.

AND IT IS AGREED and declared by the bank that the liability of the Bank to pay the said amount whenever called upon by the Beneficiary shall be irrevocable and absolute and the Bank will not be entitled to dispute or inquire into whether the Beneficiary has become entitled to forfeit the said amount as earnest money (or as security deposit) under the terms of the said contract or not and entitled to claim the same or not or whether the said bidder have committed any breach of the said contract/ RFP/ Tender document or not or whether the Beneficiary is entitled to recover any damages from the said bidders for breach of terms thereof or not.

Any such demand made by the Beneficiary shall be binding and conclusive as regards amount due and payable by the bidder to the Beneficiary. And the Bank undertakes to pay unconditionally on written demand without demur and the claim of beneficiary shall be conclusive and binding as to the amount specified therein.

AND it is further agreed and declared by the Bank that any waiver of any breach of any term of the said contract/RFP/Tender or any act of forbearance on the part of the Beneficiary or any time given by the Beneficiary to the bidder for carrying out and completing the work under the said contract or any modifications made in the terms and conditions of the said contract or any other act or omission on the part of the Beneficiary which could have in law the effect of discharging a surety, will not discharge the Bank.

AND it is agreed and declared that this guarantee will remain in force until the time fixed in the said contract/RFP/Tender or until the expiration of any extended time for such completion and shall be valid for a period of six months from the date hereof i.e. the guarantee shall be valid upto ……

AND it is agreed and declared that this Guarantee will be irrevocable and enforceable even if the bidder's company goes into liquidation or there is any change in the constitution of the said Company or management of the said Company and shall ensure to the benefit of its successors and assigns and shall be binding on the successors and assigns of the Bank.

Notwithstanding anything contained herein:

The liability of the Bank under this Bank Guarantee shall not exceed Rs. XXXXXX/-. (Rupees XXXXXX only).

This Bank Guarantee shall be valid up to _____.

Bank is liable to pay guaranteed amount or part thereof under this Bank Guarantee only and only if beneficiary serve upon as a written claim or demand on or before _____ (date of expiry of the Guarantee).

IN WITNESS WHEREOF the Bank has put is seal the day and year first hereinabove written. Signed, sealed and delivered by Mr……

For and on behalf of the Guarantor Do so and

to affix the seal of the Bank, in the presence of …….

Annexure 05 – Undertaking Letter

To

The Chief Operating Officer,
The Nainital Bank Limited,
Head Office, Seven Oaks Building
Mallital, Nainital-263001

Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Integration, Training & Maintenance of Fraud Risk Management System

1. Having examined the Tender Documents including all Annexure and Appendices, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply, deliver, implement and commission ALL the items mentioned in the 'Request for Proposal' and the other schedules of requirements and services for your bank in conformity with the said Tender Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Tender.
2. If our Bid is accepted, we undertake to comply with the delivery schedule as mentioned in the Tender Document.
3. We agree to abide by this Tender Offer for 180 days from date of bid opening and our Offer shall remain binding on us and may be accepted by the Bank any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. a) We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

   b) Commission or gratuities, if any paid or to be paid by us to agents relating to this Bid and to Contract execution, if we are awarded the Contract are listed below.

      i. Name and Address of the Agent - ……

      ii. Amount and Currency in which Commission paid / payable - …….

      iii. Purpose of payment of Commission (If commission is not paid / not payable indicate the same here) - .....
6. We agree that the Bank is not bound to accept the lowest or any Bid the Bank may receive.
7. We certify that we have provided all the information requested by the bank in the format

requested for. We also understand that the bank has the exclusive right to reject this offer in case the bank is of the opinion that the required information is not provided or is provided in a different format.

Dated this..... by 20

Yours faithfully,

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

(This letter should be on the letterhead of the Vendor duly signed by an authorized signatory)

Annexure 06 - Comments Format

[Please provide your comments on the Terms & conditions in this section. You are requested to categorize your comments under appropriate headings such as those pertaining to the Scope of work, Approach, Work plan, Personnel schedule, Curriculum Vitae, Experience in related projects etc. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.]

Name of the Respondent:

Contact Person from Respondent in case of need.

Name :

Tel No: e-Mail ID:

Sr. No.	Page #	Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation
1				
2				
3				
4				
5				
6				
7				
8				
9				

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone # Date:

Annexure 07 – Conformity with Hard Copy Letter

(***This letter should be on the letterhead of the bidder duly signed by an authorized signatory***)

To

The Chief Operating Officer,

The Nainital Bank Limited,

Head Office, Seven Oaks Building

Mallital Nainital-263 001

Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System

Further to our proposal dated ……., in response to the Request for Proposal ……. (Bank's tender No. hereinafter referred to as **"RFP"**) issued by The Nainital Bank Limited (**"Bank"**) we hereby covenant, warrant and confirm as follows:

The soft-copies of the proposal submitted by us in response to the RFP and the related addendums and other documents including the changes made to the original tender documents issued by the Bank, conform to and are identical with the hard-copies of aforesaid proposal submitted by us, in all respects.

Yours faithfully,

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

Annexure 08 – Conformity Letter

(***This letter should be on the letterhead of the bidder duly signed by an authorized signatory***)

To
The Chief Operating Officer,
The Nainital Bank Limited,
Head Office, Seven Oaks Building
Mallital Nainital-263001

Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System

Further to our proposal dated ……., in response to the Request for Proposal ……. (Bank's tender No. hereinafter referred to as "RFP") issued by Nainital Bank ("Bank") we hereby covenant, warrant and confirm as follows:

We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents issued by the Bank shall form a valid and binding part of the aforesaid RFP document. The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.

Yours faithfully,

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

Annexure 09 – Letter of Undertaking from OSD / OEM

(***This letter should be on the letterhead of the OEM / OSD / Manufacturer duly signed by an authorized signatory***)

To

The Chief Operating Officer,

The Nainital Bank Limited,

Head Office, Seven Oaks Building

Mallital Nainital-263001

Sub: **RFP for Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System**

Sir,

We …… (Name of the OSD / OEM) who are established and reputable manufacturers / developers of …… having factories at ……, …… and …… do hereby authorize M/s …… (who is the vendor submitting its bid pursuant to the Request for Proposal issued by the Bank) to submit a Bid and negotiate and conclude a contract with you for supply of …… which are manufactured / developed by us against the Request for Proposal received from your Bank by the Bidder and we have duly authorised the Bidder for this purpose.

We undertake to perform the obligations as set out in the RFP in respect of such services and hereby extend our support and services through M/s. …… during the 5 year contract period as per terms and conditions of the RFP.

We assure you that in the event of M/s …… not being able to fulfill its obligation as M/s ……vendor in respect of the terms defined in the RFP, … ……(OEM / OSD Name) would continue to meet these either obligations directly or through alternate arrangements without any additional cost to the Bank.

Yours Faithfully

Authorised Signatory

(Name:

Phone No. Fax Email)

Annexure 10– Undertaking of Information Security

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

To

The Chief Operating Officer,

The Nainital Bank Limited,

Head Office,Seven Oaks Building

Mallital Nainital-263001

Sir,

Sub: Request for Proposal for Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System

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

Yours faithfully,

Authorized Signatory
Name:

Designation:

Vendor's Corporate Name Address

Email and Phone #

Annexure 11- Technical requirement (Broad Scope of Work)

A. Project Scope

Bank will award the contract to the successful vendor and the vendor should deliver the service with the following scope:

1. Broad Scope of Work

The Vendor is required to supply, configure, customize, maintain and support solution for FRMS. The scope of work would include design, supply, implementation, customization, integration, testing, documentation, training, warranty support and post warranty maintenance support for all the solution components including software/database/licenses/tools required for the fulfilment of the scope for a period of 5 years. The 5-year period consists of warranty and subsequent AMC/ATS period, from the date of implementation.

The proposed solution should be implemented at Bank's premise in High Availability mode, along with DR and a minimum uptime time of 99.9 %.

The FRMS product solution will provide enterprise wide fraud detection and prevention covering the risks associated with the below mentioned indicative list of channels and applications under online and/or offline mode. The solution should cover prevention and detection of frauds at different process stages of the below mentioned applications and channels for all types of transactions such as card present, card not present, financial and non-financial transaction etc.

Online Mode: - The Fraud detection is to be done on real time basis. The authorization/decline of the In-flight transaction should not affect performance of the source systems. Real time monitoring and actioning on transactions pertains following products: -

a. Core Banking
b. Internet Banking
c. Mobile Banking
d. Debit card.
e. POS (Point of Sale)
f. Cash Deposit machines / Cash Recyclers
g. Internet Payment Gateway and E-commerce Transactions
h. FI (Financial Inclusion) Gateway
i. IVR (Interactive voice response)
j. UPI
k. NACH
l. PFMS
m. Any other delivery channel introduced by the Bank during the contract period

Offline Mode: - The Fraud detection is done post facto and the decision should not have any impact on the in-flight transaction. Offline monitoring/Near Real Time alert management and actioning on transactions pertains to following channels / products:-

Branch Banking (Domestic)

a. All Deposits Products

b. Loans
   i. Corporate Loans
   ii. Retail Loans
   iii. MSME Loans
   iv. Agriculture/Priority Sector Finance

c. Trade Finance / Non-Fund Credits
   i. Bank Guarantees
   ii. Letter of Credits
   iii. Bill Finance (Bill discounting, Bill purchase etc.)

d. Remittances (NEFT, RTGS)

Other Banking products

- Service Branch (Cheque Processing / ECS processing) Operations
- Treasury Operations
- Financial Inclusion Banking
- SFMS events
- Cyber Incidents

Internal Frauds (Employee initiated /involvement)

The Bidder is expected to integrate the solution with the existing transactional and other systems deployed by the Bank without impacting the performance of the source systems.

The major systems deployed for various channels are as under: -

- Infosys Finacle Core Banking Software, Delivery channel integrator is Connect 24 of Finacle.
- Infosys Finacle Internet Banking Solution
- ATM Switch
- Mobile Banking Solution
- POS Switch
- Treasury Application
- Financial Inclusion solution / Gateway solution

Proposed Solution should be able to integrate with different channels such and their supportive internal systems such as E.g. Debit card, POS, CBS system, AML solution, HRMS system, Cheque Fraud, Online Banking products and services, other software relating to products and services offered by Corporate Banking, Retails Assets and Liabilities, Branch Banking, Treasury etc. and also support external systems like CIBIL, UDS, CERSAI, CRISIL etc. as per requirement of the Bank for Fraud risk management. The solution should have proven integration capabilities with the CBS and bidder should ensure that the FRM solution does not have a performance impact on the CBS or any other channel.

The proposed solution should support high disk IOPS (Input Output Operations per Second) to meet the banks requirement in terms of performance. Proposed software should support open modular architecture proving following broad level capabilities:

- Detection & Rule Engine
- Case Management & Workflow
- Scoring

- Analytics
- Data Management
- BI (Business Intelligence) & Reporting
- Integration & Interface
- Integrated Fraud Management
- Forensic Support

(a) Internet and Mobile Banking

The proposed solution should be able to integrate with Finacle CDCI–/ Connect 24 channel integrator to monitor Internet and mobile banking transactions with minimal/no support from the actual CBS bidder. Solution should also support new versions of Finacle CDCI.

- The proposed solution should monitor and detect frauds for all pre-login, login and post login related transactions.
- The proposed solution should support advanced IP geo-location capability to detect IP Country, IP City, Proxy IP and zone hopping.
- The proposed solution should support site authentication capability with personalized images and phrases.
- The proposed solution should support wide range of 2FA techniques including SMS/Email OTP, software tokens, hardware tokens, transaction signing tokens, PKI certificates & Digital Signature certificate.
- The proposed solution should not require any download or installation by the end user and should support all types of browser and operating systems environments on all devices e.g. Personal Computers / Laptops / Smart phones/ other devices.

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
- Average Daily/Weekly/Monthly Funds Transfer amount / frequency by payee / biller
- Preferred Transaction hour
- Proposed solution should support IPV6 addressing.

(b) Transaction Monitoring for Core banking transactions

- The proposed solution should be able to integrate with Finacle CBS with minimal/no support from the actual CBS bidder. Solution should also support new versions of Finacle CBS.
- The proposed solution should have the capability to detect and block/hold suspicious fraudulent core banking transactions.
- The proposed solution should not impact the performance of Finacle core banking

application and other applications.

- The proposed solution should be able to monitor both financial and non-financial transactions and detect frauds from core banking transactions.
- The proposed solution should support both transaction monitoring and fraud prevention/transaction capability for core banking transactions.
- The proposed solution should provide pre-packaged scenarios or have the flexibility to create such scenario with minimal efforts as and when required to detect various branch banking and employee frauds including account take over, embezzlement, nepotism, suspicious inquiries etc.

(c) Real-Time Fraud Prevention for Payment Card transactions

a. The proposed solution should be able to integrate with Connect 24 channel integrator to monitor Debit card transactions across ATM, POS, and E- Commerce channels with minimal/no support from the actual CBS bidder. Solution should also support new versions of Finacle.

b. The proposed solution should support payment card fraud prevention against skimming, counterfeit cards, lost and stolen cards, Mass card compromise, sudden surge and anomalous behavior, zone hopping.

c. The proposed solution should be able to combat both card present and card not present frauds in real-time.

d. The solution should provide pre-packaged scenarios and scoring models or have the flexibility to create such scenarios and models with minimal efforts as and when required for debit cards and credit cards.

e. The proposed solution should have capability to detect common point of compromise (CPC) for compromised ATM, POS, and Merchants. Proposed Solution should be able to detect merchants/ATMs with common point of compromise (CPC) and be able to add these entities into blacklists.

f. The proposed solution should support customer looped fraud prevention capabilities where customers can set their own rules regarding their debit card usage using mobile banking or internet banking interface. Sample customer defined rules/policies include: Block transactions from particular country, Block transactions from particular channels for a country, Block specific channel transaction exceeding a threshold amount etc.

g. Proposed Solution should support out of the box behavior profiles including but not limited to:

(i) Card holder profiles

(ii) Preferred ATM machines

(iii) Preferred Merchants

(iv) Preferred Merchant Category Codes preferred Country /City

(v) Preferred Transaction hour for ATM, POS, E-Commerce

(vi) Preferred Currency for purchase - Average Daily/ Weekly/ Monthly/ Quarterly / Season based transaction amount by channel (for domestic transactions)

(vii) Average Daily/Weekly/Monthly/Quarterly/Season based transaction frequency by channel (for domestic transactions)

(viii) Proposed Solution should provide pre-packaged scenarios and custom predictive scoring models to detect and prevent traditional and emerging fraud attacks like velocity checks, data

breach and mass card compromise, zone hopping, customer state change and unusual transactions, sudden surge deviating from usual card holder or merchant profile, cross channel frauds, overseas card compromise and watch lists monitoring.

(ix) Proposed Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.

(x) Proposed 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.

Additionally, the Bidder will be responsible for

a. The end to end Implementation of the solution (FRMS) including integration with various systems to meet the requirement of Detection, Monitoring and Prevention of the Fraud
b. The end to end software development life cycle of the FRM Solution
c. Customization, parameterization and implementation of application software and solutions
d. Facilities management services at the DC and DR
e. Hand-over successfully either to the bank or any vendor appointed by the bank at the end of the agreed upon contract period
f. Setting up a IT Service desk

The services offered in contract period must be in conformance with the specifications supplied in the Technical Specification. During this period, the Bidder will be responsible for the patch application / bug fixing / replacement / support of all software supplied under this tender.

2. General Solution Requirement

2.1. Bank intends to implement fraud risk management solution covering core banking, delivery channels and other banking applications across the entire bank.

2.2. The proposed solution should be able to comply with various RBI and other regulatory guidelines related to electronic payments.

2.3. Implementation of the FRMS solution should be completed within 9 months of the acceptance of order in a phased manner.

2.4. The license for the solution to be Enterprise wide perpetual level for all the modules offered without any constraint on the number of branches / customers or users for the Bank‘s operations in India.

2.5. The bidder should regularly track alerts generated by system as well as global feeds and accordingly advise the Bank about global security threats and vulnerabilities. Bidder should advise the bank for upgrades /changes in the security infrastructure of the Bank against evolving threats and responsibilities.

2.6. The bidder should install, integrate and customize proposed solution with Bank’s existing Core Banking System (Finacle), Internet banking application (Finacle eBanking from Infosys), Mobile Banking application, Bank’s ATM switch, Debit cards and other transaction systems/ delivery channels etc. without hampering the routine operations of the bank. The bidder should accomplish the job in coordination with existing System Integrator of the CBS and Internet Banking solution and other applications. Also, the proposed solution should support new versions of all the applications.

2.7. Bidder will integrate different channels/systems existing and introduced in the Bank within contract period in the Fraud Risk management (FRM) Solution without any cost. Integration required to the Bank environment has to be done at no extra cost and will be

the sole responsibility of the Bidder including minor enhancements.

2.8. Bidder should build required interfaces, if any, for delivery channels and CBS at no extra cost.

2.9. The FRM Solution should have the capability of supporting security framework in terms of authentication, multi-level authorization, auto log-off, password control, single sign-on audit. The solution should allow administrators to implement access management in a granular manner. The proposed solution should be able to integrate with banks existing authentication 2FA infrastructure and Biometric authentication for stronger authentication.

2.10. 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, etc.

2.11. The solution should support balancing the ratio false positive/negative ratio to reach manageable thresholds. By way of using out of box analytics capabilities. Analytics Capabilities need to be reviewed/ calibrated periodically.

2.12. Proposed Solution should provide risk score model which shall identify activities in the account that shall score the increase in the risk parameter and provide alerts

2.13. The system should be capable of managing Fraud risks proactively and also should be able to prevent the Fraud risks at the detection stage itself.

2.14. The system should be provide of appending/converting the structured/semi structured/unstructured image based information into digital data for effective use of information in identifying various risks on a proactive online / real time basis. The system should be capable of perform high level data analytics at any levels of permutation and combination.

2.15. The system should be capable of generating any levels of dashboards and MIS to meet the requirements of individual user / Unit level / Management level / Product & Process level / all demographic level / All outlier levels / All regulatory reporting levels.

2.16. The proposed solution should provide the capability to detect, discover, prevent and investigate the frauds in real time not only restricted to only one channel but across all the channels mentioned i.e. CBS, ATM, Internet Banking, Mobile banking , Debit Card and POS.

2.17. Solution should support automated interactive outbound call based alerts on 24X7 basis to intimate and confirm with customer in case of high risk transaction.

2.18. Solution should support automated interactive SMS based alert facility on 24X7 basis to intimate and confirm with customer in case of high risk transaction.

2.19. Solution should have an interactive mobile alerting and payment platform that provides a flexible interface between mobile channels and transaction systems. It should be used for transaction push as well as pull services and use SMS, Email, mobile browser, voice, or applications as delivery platform. The system should support the receipt of a request via any mobile channel and connects with a range of host systems to process. The result should be communicated back to the originator as well as trigger a message to the proposed solution. Push data feeds should be obtained from different channels which will be processed in a business flow and should be resulted in alert messages to the users.

2.20. The bidder should take care of all aspects of Installation on existing set-up, De- Installation,

Configuration, Re-configuration, enhancements, updates, upgrades, problem analysis, on–site, as well as off-site support to ensure smooth operations during and post implementation till end of contract period.

2.21. Bidder will have to ensure the troubleshooting in all forms like technical, administrative and customer related issues etc.

2.22. The proposed solution should be able to monitor and detect frauds in real-time for all channels and near real time for CBS.

2.23. The proposed solution should have the capability for cross-channel fraud monitoring and prevention.

2.24. The proposed solution should be provided with High availability within the primary site and replication of configuration, history data, polices etc between primary site and DR site. There should be synchronization between DC and DR under bank's specified Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

2.25. To meet the RTO, the bandwidth requirement has to be mentioned in the technical bid.

2.26. The bidder should also build a dedicated infrastructure for development/testing.

2.27. Overall scope must ensure full coverage of 24*7 monitoring and fraud detection for integrated channels and products.

2.28. The proposed solution should provide robust fraud detection and risk scoring capabilities using following approach but not limited to as below:

- Advanced rule/scenario based detection
- Identity Resolution
- Dynamic Behaviour Profiling and anomaly detection
- Machine Learning based Predictive Scoring models

2.29. The proposed solution should provide pre-packaged scenarios or have the flexibility to create such scenario with minimal efforts as and when required for multiple products and channels.

2.30. The proposed solution should provide web based scenario authoring tool to configure new fraud schemes as and when required.

2.31. The proposed solution should allow configuring various business policies like approve/decline/challenge/hold transaction based on the fraud risk score.

2.32. The proposed solution should provide advanced case management system with rich client software for link analysis and visualization of complex networks that can be integrated across source systems for case investigation.

2.33. Proposed case management system should support configurable work flow based on the case type and built-in auto case routing mechanism.

2.34. The FRM solution should provide open APIs so that the Bank's different applications can be integrated with the FRM solution.

2.35. Proposed Solution should conform to all regulatory, statutory, legal acts and rules including IT Act, 2000 (Amended 2011).

2.36. Proposed advanced case management tool should be integrated with the case

investigation, link analysis and visualization tool for the case investigation.

2.37. Proposed case management solution should support case escalation feature based on business policies configured.

2.38. The proposed solution should support watch list management for various black lists and white lists.

2.39. The proposed solution should support entity link analysis tool to detect organized fraud rings and collusions.

2.40. The proposed entity/network link analysis tool should support both static link analysis based on customer/account demographics and dynamic link analysis based on transaction parameters.

2.41. The proposed solution should provide complete evidences for why a transaction was declined/hold by the fraud management system.

2.42. The proposed solution should provide complete audit trail.

2.43. The proposed solution should support encryption and digital signature feature.

2.44. The FRM solution should support virtual keyboard.

2.45. The proposed solution should support built-in maker checker functionality to ensure dual commit to critical system changes.

2.46. The proposed solution should provide MIS dashboard and reports for tracking fraud cases, investigators" performance and system performance.

2.47. Bidder will have to ensure the troubleshooting in all forms like technical, administrative and customer related issues etc.

2.48. Bidder should provide SLA based services and the SLA tracking system as well as for maintaining operational workflow.

2.49. The bidder should provide enterprise case management for viewing of all the channels

2.50. The FRMS solution must provide open APIs for integration with different applications of the Bank and its customers.

2.51. The FRMS should support online/ real-time comprehensive and customizable management dashboard.

2.52. The FRMS solution should provide audit trails and logs of all its functions/processes.

2.53. The FRMS solution will include middleware, training, third party utilities and installation, testing, migration, providing requisite interfaces and provide technical support for a period of five years. The five-year period consists of warranty and subsequent AMC/ATS period, from the date of implementation.

2.54. The Vendor should provide diagrammatic/ pictorial representations for complete details of the hardware, software and network architecture of the solution offered, including the project plan for going live. The Vendor should also provide security set- up of the solution and its layers of risk identification and mitigation.

2.55. The Vendor shall do proactive monitoring and capacity planning at regular intervals and advise the Bank about the hardware and software upgrades. However, there should not

be any additional cost to the Bank for any hardware or software upgrade during the contract period as the Bank may use existing IT infrastructure or procure separately the required infrastructure based on the sizing proposed by the Vendor. As part of the technical solution, the Vendor must provide the complete IT infrastructure details like Server, Operating System, Database, Storage Capacity and other related requirements. In the event the sizing proposed by the Vendor does not meet the performance/ service levels of the Bank, the Vendor will at their cost carry out the necessary upgrades/ replacements. The Bank has the right to deduct/ recover from the Vendor, the required additional expenses which the Bank may incur on account of such upgrades/ replacements.

2.56. The Vendor should provide a separate Test/ Development/ UAT environment.

2.57. For every software including any third party software before software/ service become operational, the Vendor must provide scope of work, user manuals, installation manuals, operation manuals, design documents, process documents, technical manuals, functional specification, software requirement specification, system configuration documents, system/ database administrative documents, debugging/ diagnostics documents, test procedures and any other documents etc.

2.58. The Bidder, at the minimum, following documentation on the following for the implementation under FRMS:

- Business Requirements Document
- Detailed functional and technical scope document
- Functional Requirement Specification Manual
- Solution Architecture
- Proposed Project Plan
- Strategy Document for Testing, Training and Acceptance
- Software source code and customization documentation
- Integration Testing Plan
- System Performance Benchmarks
- Test Specifications
- User Acceptance Reports
- Maintenance Document
- Configuration and User Manuals
- Release Management Document
- Training Plan
- User Training Manuals
- Licenses for all the software components
- DR Document
- Detailed Mapping Details
  - Interfaces
  - Case & Alert Creation
  - User Defined variables

2.59. Application Documentation: The following minimum documentation (hardcopy and soft copy) for all the proposed software applications/ hardware components must be made

available:

- General functional description
  - Set up and installation Manual
  - User Manual
  - System administrator Manual
- The Bidder and the bank will jointly maintain a repository of all project artifacts created as part of the project at the Bank's premises including but not limited to project plan, architecture, design, code samples. Should there be a termination of contract this entire repository needs to be handed over to the bank by the Bidder as part of contract termination. The security, integrity and data protection of this repository, which is established in the Bank's premises, is the responsibility of the Bidder.
- The Bidder will be expected to deliver to the Bank for each installation site, one (1) physical copy and one (1) electronic copy of documentation for each of the deliverables and online context-sensitive help module included in the software to enable the Bank's personnel to use and understand the operations of the deliverables. The Bank may make additional copies of the Bank- specific Documentation for their internal use

2.60. The Vendor should also provide documents related to Review Records/ Test Bug Reports/ Root Cause Analysis Report, list of all product components, list of all dependent/ external modules and list of all documents related to traceability of the product as and when applicable. The Vendor should also provide the MIS reports as per requirement of the Bank. Any level/version changes and/or clarification or corrections or modifications in the above mentioned documentation should be supplied by the Vendor to the Bank free of cost in timely manner.

2.61. The FRMS solution must include pre and post-implementation support.

2.62. The FRMS solution must provide the Bank with escrow of the application software.

2.63. The FRMS solution must benchmark with the market if desired by the Bank.

2.64. The Vendor must provide FRMS Services to enrich/enhance each document with additional meta-data fields to ensure end-to-end audit trail and tracking.

2.65. The FRMS solution developed or customized should follow a standard development process to ensure that it meets functional, security, performance & regulatory requirements of the Bank, RBI and other regulatory authorities.

2.66. All the patches/fixes, version upgrades of all the software components released by the Principal OEM during the contract period should be provided. The Vendor should ensure implementation of all the patches/ fixes and version upgrades in the production environment to the latest version during the contract period.

2.67. The Vendor will ensure seamless migration of the application and solution after expiry of contract period, if the Bank selects another vendor after the contract period or during the contract period due to any reason.

2.68. If the Bank desires to upgrade to higher version of database or hardware, the Vendor shall be required to comply with the Banks requirement. The FRMS solution should support the database and hardware version which are supported by OEM. The Bank will take care of

hardware and database upgrade activity. The Vendor has to ensure that the application should be compatible with hardware and database etc. without any additional cost.

2.69. System integration testing will be followed by user acceptance testing, plan for which has to be submitted by the vendor to the Bank. The UAT includes Functional tests, Resilience tests, Benchmark Comparisons, Operational tests, Load tests etc. The Bank 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 the Vendor. The Vendor should carry out other testing like resiliency / benchmarking / load etc. and submit the result log for all testing to the Bank.

2.70. If there is any core banking system upgrade, then it is the Vendor's responsibility to ensure that the integration with the core banking system is provided without affecting the normal course of business.

2.71. The FRMS solution / software developed or customized should follow a standard development process to ensure that it meets functional, security, performance & regulatory requirements of the Bank.

2.72. The Vendor should comply with Bank's IS Security policy in key concern areas relevant to the RFP. Some of the key areas are as under:

- Responsibilities for data and application privacy and confidentiality
- Responsibilities on system and software access control and administration
- Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to the Vendor
- Physical Security of the facilities, wherever required to be provided by the vendor
- Physical and logical separation from other customers of the Vendor, wherever required to be provided by the vendor
- Incident response and reporting procedures
- Password Policy of the Bank
- Data Encryption

Security requirement of the Bank will be shared with the successful bidder.

2.73. Backup System: The Vendor will be responsible for Backup of application and the database as per the requirement of the Bank.

2.74. Test & Training: Exclusive Test & Training environment should be made available outside production area in the respective DC.

2.75. Any impact on Production, Test & Development and Training environment sizing has to be taken into account by the bidder during the contract period and the bank will not be liable to pay for any additional cost. However, the bidder should right size the solution to meet the requirements provided in this RFP for the contract period of 5 years. In case the RFP requirements are not met, then the selected bidder has to provide additional components required to meet the RFP requirements, at no additional cost to the bank

2.76. The AI and ML capabilities of the solution should be clearly demonstrated by the selected bidder.

2.77. FRM setup/infrastructure may be subjected to audit from Bank and/or third party and/or

regulatory body. It shall be responsibility of the Bidder to cooperate and provide necessary information and support to the auditors with respect to the FRM project. The Bidder must ensure that the audit observations are closed on top priority and to the satisfaction of the Bank, regulator and its appointed auditors. Extreme care should be taken by the Bidder to ensure that the observations do not get repeated in subsequent audits. Such noncompliance by Bidder shall attract penalty.

3. Hardware Sizing and Performance Required

The vendor should Design & Size the hardware required at DC & DR. The Vendor is supposed to provide the complete hardware requirement for the end-to-end functioning of FRMS solution. The Vendor has to provide necessary requirement of infrastructure (Servers / OS / Database / Middleware etc. which are required for the system) as under:

1. Data Centre (DC) - Production
2. Data Centre (DC) - Test, Development and Training
3. Disaster Recovery Site (DR)

The Vendor must provide requirement of optimal size of the Hardware, Operating System, Database, Middleware etc. keeping in view the current average and peak volume of transactions and to extrapolate the same for the full TCO period (i.e. 5 years). The propose infra shall be optimized in the solution document. Oversizing of infra requirement will also be evaluated while doing the evaluation of bidders.

The vendor must provide requirement of Application Performance Monitoring (APM) tool of the monitoring of the transactions and the system performance, real and near to real time transactions as well as for capacity planning.

The proposed solution should support the existing customer base /transaction base on each of the channel including CBS and must support scalability to add additional future growth without the need to discard the earlier set-up. The present customer base/transaction base with the channels are as below: -

S.No	Channel/ e-Channel	User Base (In Lacs)	Transactions /Year (In Lacs)	Expected Growth of Transactions/ Year	Expected Growth of user base/ Year
1	CBS	12	1700	30%	10%
2	ATM card holders	3	15	10%	20%
3	Internet Banking	.2	1	50%	20%
4	Mobile Banking	0	In Process	50%	50%

During the agreement period, if at any stage, it is found that the solution provided by the Vendor is not able to give the requisite performance as per the sizing parameters the Vendor shall have to provide additional hardware, software without any additional cost to the Bank. The hardware proposed for the FRMS solution as part of this RFP should not exceed 70% of CPU(s), Memory(s), Hard Disk(s) utilization levels at any given point in time during the TCO Period.

The Data replication should happen from Primary site to DR site on real time to keep them in sync. The Vendor is also required to conduct at least one DR drill in a quarter.

1.1. Projected Volume of Transactions:

Average yearly transaction* volume (in Lac)

Transaction Channels	Year 1	Year 2	Year 3	Year 4	Year 5
UPI	600	720	864	1036.80	1244.16
		20%	**20%**	**20%**	**20%**
Net Banking	1	1.5	2.25	3.38	5.07
		50%	**50%**	**50%**	**50%**
ATM/POS/ECOM	15	16.5	18.15	19.97	21.97
		10%	**10%**	**10%**	**10%**
Mobile Banking(In Process)	20	30	45	67.5	101.25
		50%	**50%**	**50%**	**50%**
AEPS	1	1.5	2.25	3.38	5.07
		50%	**50%**	**50%**	**50%**
IMPS	1	1.5	2.25	3.38	5.07
		50%	**50%**	**50%**	**50%**
RTGS	1	1.1	1.21	1.33	1.46
		10%	**10%**	**10%**	**10%**
NEFT	24	31.2	40.56	52.73	68.55
		30%	**30%**	**30%**	**30%**
CBS (Branch Transactions)	200	204	208.08	212.24	216.5
		2%	**2%**	**2%**	**2%**

Average yearly transaction* volume (in Lac)

CBS (All Transactions)	800	1040	1352	1757.6	2284.88
		30%	**30%**	**30%**	**30%**

***Transaction** - Every request to proposed solution from Bank's System/ Customer and communication of final decision back to Bank's System/ Customer is considered as one transaction; all intermediary hops are considered as part of the same transaction including reversals.

Performance & Volume Metrics of Case Management Solution	**Estimated No of concurrent users:** Year 1-5: 100 users **Estimated No of total users:** Year 1-5: 200 users
Expected Response Time	Server-side response time: < 100 ms Effective TPS: 1000

1.2. Performance testing and Validation methods

The proposed solution should be readily measurable with the following performance Benchmarks and Performance testing methods

Performance Benchmarks:

- Transaction Processing Speed: Measured in transactions per second (TPS).
- Rule Evaluation Time: Average time taken to evaluate a rule.
- Alert Generation Latency: Time taken from detection to alert generation.
- System Response Time: Overall system response time under different load conditions.
- Data Processing Efficiency: Speed of data ingestion, transformation, and loading.
- Scalability: Ability to handle increased transaction volumes and data growth.

Performance Testing Methods:

- Load & Stress Testing: Simulating increased user loads to identify the system's performance under stress.
- Endurance Testing: Simulating sustained user load over an extended period to assess system stability.
- Volume Testing: Tests the system's ability to handle large volumes of data.

Validation Methods:

- Benchmark Comparison: Comparing test results against predefined performance benchmarks
- User Acceptance Testing (UAT): Feedback provided from end-users will be utilized for performance testing.

4. Project Timelines Deliverables

The proposed solution should be implemented in 9 months of period from the date of placing purchase order. The implementation should be carried out in three phases:

Phase – I: The vendor must implement the FRM solution and interface with CBS, Debit Card/POS/ E-Commerce,Net Banking,Mobile banking,SMS and Email gateway in this phase. All other readily available functionalities with CBS data should be available. Phase - I Go-Live is in 3 months from the start of implementation.

Phase – II: All other readily available functionalities in India and interfaces with other systems to cover Asset side frauds, case management, NEFT/RTGS,UPI,IMPS,AePS, Access of System to be available up to identified Regional Centres. Phase - II Go-Live is in 6 months from the start of implementation.

Phase – III: All functionalities covering all types of frauds as per RFP Customizations need to be completed in this phase including Call Centre & IVRS(All Channels), Behavioral Biometric Application Integration, branch transactions* Phase-III Go-Live is in 9 months from the start of implementation.

*Branch Transactions (including monitoring of Internal Accounts, Deposit accounts, Loan accounts, Staff Accounts, New Accounts, Money mules, CTS, NACH, PFMS, Open API etc.)
Various external Feeds to be consumed/provided as & when required

5. Monitoring and Audit

- Compliance with security best practices may be monitored by periodic computer security audits / Information Security Audits performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The Vendor must provide the Bank access to various monitoring and

performance measurement systems. The Vendor has to remedy all discrepancies observed by the auditors at no additional cost to the Bank.

- For service level measurement, as defined in SLA, data recording is to be captured by the industry standard tools implemented by the Vendor. These tools should be a part of the proposed solution.

6. Technical Scoring Sheet:

Sl No.	Particulars	Yes(Y)	Customizable (C)
1	Proposed Solution should have ability to failover without/with least manual intervention.		
2	Proposed Solution should replicate the data between DC & DR in real time basis or as required by the bank.		
3	Proposed Solution should store historical incidents/alerts onsite to correlate future transactions.		
4	Proposed Solution should integrate with all existing delivery channels of the Bank as specified in "Detailed Scope of Work", Annexure 11 above.		
5	The proposed solution should take/give feeds from/to various applications of the Bank as specified in in "Detailed Scope of Work", Annexure 11 above above.		
6	For Customer Outreach, the proposed FRMS Solution shouldintegrate with Bank's various authentication/ gateway solutions as specified in in "Detailed Scope of Work", Annexure 11 above above.		
7	Proposed Solution (System/Application) Should maintain Audit Logs of all user activities including User ID, Date/Time, IP Address, Terminal ID, etc.		
8	Should conform to all regulatory, statutory, legal acts and rules including IT Act, 2000 (Amended 2008).		
9	Proposed Solution should have an integrated case management system where the alerts get triggered basedon the real-time transaction monitoring performed.		
10	Proposed Solution should enable real-time case creation for any fraud/non-compliance patterns identified by the real-time transaction monitoring engine.		
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.		
12	Real-time cases should get triggered in the right type of project/queue as per the categorization.		
13	Proposed Solution should have access controls available to establish groups of authorized Bank users with different privilege levels.		
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		

15	Proposed Solution should have provision for configuration of workflow for alerts/cases as per bank's operational process requirements		
16	Proposed Solution should have ability to route and assign cases to the right set of investigators based on pre-defined case routing Logic.		
17	Proposed Solution should have ability to define roles and user groups and assign privileges.		
18	Proposed Solution should provide complete evidence and list of transactions that cause a scenario match and alert.		
19	Proposed Solution should have ability to define and categorize the different types of frauds/non- compliance.		
20	Proposed Solution should have Auto and manual linking of alerts to parent entity case.		
21	Proposed Solution should configure for Alerts to be sent to appropriate users via SMS or email.		
22	Proposed Solution should have ability to manually assign alerts to users.		
23	Proposed Solution should have Built in escalation matrix to assign alerts automatically to stake holders for review and assessment.		
24	Proposed Solution should have facility for auto-update (list of reasons) of user comments while closing alerts.		
25	Proposed Solution should have ability to attach a doc, image, data from other systems to an alert.		
26	Proposed Solution should have ability to export the case reports.		
27	Proposed Solution should have ability to flag an alert based on the pre-defined criteria (e.g. false positives, suspicion, type of fraud).		

28	Proposed Solution should have ability to mark an entity (customer, account, device, IP etc.) to a watch list.		
29	Proposed Solution should have ability to send feed back to the fraud prevention engine to reduce false positives and increase fraud prevention rate.		
30	Proposed Solution should be capable of generating Real time alerts using artificial intelligence/ machine learning.		
31	Proposed Solution should Support complete audit trail for each user action throughout the case life cycle.		
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.		
33	Proposed Solution should have ability to view all alerts corresponding to a particular customer/account under a single parent case.		
34	Proposed Solution should have ability to resolve alert into one of the final states e.g. confirmed fraud, false positive etc.		
35	Proposed Solution should have ability to categorize the confirmed fraudulent case into one of the categories as per RBI fraud reporting categorization		
36	Proposed solution should have ability to drag and flag suspicious transactions on digital platform.		
37	Proposed solution should generate alerts based on customer risk category and threshold limit.		
38	It should provide facility for prioritization of alerts based on scenarios requirement.		
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.		
40	Solution should support use of standard logical operators (eg: AND, OR, NOT etc) in all Real time Authorization of Rule conditions.		

41	Solution should support use standard arithmetic operators (e.g.: >, <=, = etc) in all Real time Authorization Rule conditions.		
42	Rules engine should be able to create / modify exclusion criteria, within a rule, to route activity to an exclusion queue.		
43	Rules engine should enable the users to interact with recent data to identify the transaction patterns during the day.		
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.		
45	System should support to single click blocking of all the transaction channels.		
46	The proposed solution should have the capability to generate Risk score based on both transaction (channel wise) and at customer profile level.		
47	The solution should have the ability for each transaction to be evaluated by every rule.		
48	The solution should be able to identify the rules triggered by a transaction.		
49	The solution should be able to assign weightages to the rules.		
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.		
51	The proposed solution should have the capability to create the rules based on user defined and derived variables using the transaction data.		
52	Solution should be able to handle the ISO 8583/ISO 20022/Existing XML Messages.		
53	Solution should be able to handle the Reversal messages in both ISO and XML format sent by the respective switches.		

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.		
55	The solution should have the ability to compress the data.		
56	The proposed solution should have the capabilities to integrate Open & Enterprise APIs with Banks middleware solution.		
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.		
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.		
59	Solution should have ability to define clusters using several different techniques and relations.		
60	The user access management at application level should be able to restrict the rights to delete/modify/recreate workflow steps of certain users.		
61	The proposed solution should automatically trigger alerts through Mail/SMS to concerned stake holders if there is no Heartbeat or Response from the FRMS.		
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.		
63	The Solution should support detailed Threshold Analysis, in order to fine tune alerts and reduce false positives.		
64	The solution should provide analytical capabilities for: Correlations & Regression, Network plot Decision and Tree Scenario analysis.		
65	The proposed solution should provide complete evidence for why a transaction was declined/hold by the fraud management system.		

66	The proposed solution should support built-in maker-checker functionality to ensure dual commit to critical system changes.		
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.		
68	The solution should support & leverage the knowledge of already identified historical frauds when authoring new rules.		
69	The proposed solution should have the ability for additional review(s) of case disposition based on several factors (role, tier, delegated authority, etc.)		
70	The solution should allow data to be accessed from any industry standard data source using native connectors and load the same in Memory.		
71	Solution should have the ability to consume data in the source format without any dependency from the individual switches.		
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 FRM Solution must carry out the monitoring across all transaction channels strictly based on Customer Identification Number (CIF no) only.		
73	Proposed solution should support both real time and near real time transaction processing i.e. after the response has been provided.		
74	The integration should not affect the performance of the source systems. Integration required to the Bank environment has to be done at no extra cost and will be the sole responsibility of the bidder including minor enhancements.		
75	Proposed solution should support cross-channel frauds & non- compliance prevention and detection in real-time.		
76	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.		
77	Proposed solution should support an advanced rule/scenario engine to prevent known fraudulent patterns.		

78	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.		
79	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.		
80	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.		
81	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.		
82	Proposed solution should provide the list of behaviour profiles supported in the system and necessary documentation for the same.		
83	Proposed solution should support product/channel specific fraud scoring models.		
84	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.		
85	Proposed solution should be able to correlate transactions across all the channels integrated in a real time basis and prevent cross channel frauds		
86	Proposed solution should be able to auto mark customers/accounts into various groups and watch lists based on case feedback.		
87	Proposed solution should be able to detect common point of compromise and mark those entities into blacklist/ watch lists.		
88	Proposed solution should have an option of adding customers in Blacklist and Whitelist manually/upload. These lists should be applicable across all channels.		
89	Proposed solution should support various business Policies to approve/decline/challenge/hold/delay transactions based on the hybrid fraud risk score.		

90	Proposed solution should automatically adjust the risk score of scenarios based on false positives occurrence.		
91	Proposed solution should facilitate categorization of cases based on the risk score of detected fraud pattern.		
92	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.		
93	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.		
94	Proposed solution should be able to monitor and detect both financial and non-financial transactions including various branch user exceptions.		
95	Proposed solution should be able to provide both real-timetransaction monitoring and transaction blocking/hold feature for suspicious transactions.		
96	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.		
97	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.)		
98	Proposed solution should be able to respond within a guaranteed low 100 millisec response time and should handle a Transaction Per Second (TPS) of 1000 transactions at the peak.		
99	Proposed Solution should implement enhanced authentication through various modes i.e. SMS-OTP, Email, PKI Authentication, Challenge-Question based on Transaction Scoring generated by the Solution as per Bank's requirement.		
100	Proposed Solution should provide Real-Time Dash Board & Alerts for multiple Role Based Users and based on different domains/Channels.		
101	The proposed solution should provide advanced case management system that should cover cases generated from all source channels.		

102	The case management system should be able to segregate the cases of customer across the channels.		
103	Proposed case management system should support configurable work flow based on the case type, and built-in auto case routing mechanism.		
104	Proposed case management system should have the ability to create, edit and view a case based on user permissions.		
105	Proposed case management system should have the ability to set default fields and values on screens based on case type.		
106	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.		
107	The proposed solution should be able to integrate alerts of all channels with IVRS for automatic calling.		
108	Proposed case management solution should support case escalation feature based on business policies configured.		
109	Proposed case management solution should be configurable with system based telephone diallers/auto diallers.		
110	Proposed case management solution should be able to simultaneously cater to at least 100 users without any performance bottle necks.		
111	Proposed case management solution should have the ability to be able to instantly update existing cases with fresh transaction detail.		
112	Proposed case management solution should have ability to link cases under investigation, elevate an alert into a case, add several alerts to one case.		
113	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 .		
114	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.		
115	The Case management solution UI should Mask the Debit/Credit Card details as per PCI-DSS standards.		
116	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.		
117	The bidder has to provide the hardware/system software sizing for data archival solution.		
118	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.		
119	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.		
120	Rule engine should have the ability to delete or remove workflows if they become redundant.		
121	Solution should support dashboard for rule administration to identify the rules that need optimization.		
122	Solution should have ability to alert when the false positive rate or the detection rate breaches a particular threshold.		
123	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.		
124	Reminder generation facility must be available when the case is about to breach the time frame allowed or expiry date time is getting closer.		
125	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.		

126	Vendor should be capable of integrating the proposed solution with Banks CBS and other related systems. Also any additions or new versions should be supported.		
127	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.		
128	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.		
129	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.		
130	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.		
131	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.		
132	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).		
133	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.		
134	Proposed solution should monitor specific general ledger account and identify suspicious debit/ credits in general ledger accounts based on the real time transaction monitoring.		
135	Proposed solution should be able to detect suspicious frauds & non- compliance patterns at both individual user/employee level and overall branch level.		
136	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.		

137	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).		
138	Theproposed solution should monitor Internal Accounts, Deposit accounts, Loan accounts, Staff Accounts, New Accounts , Money mules, CTS, NACH, PFMS, Account Disbursement services etc.		
139	The proposed solution should have the capability to handle the Bulk approval Payment events.		
140	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.		
141	FRMS 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.		
142	FRMS should have the ability to detect potential fraudulent accounts opened in the name of employees and indicating suspicious transactions.		
143	The proposed solution should monitor Employee or related accounts with high credit limits receiving high number of transactions.		
144	The proposed solution should monitor Accounts with high balances that are closed by an employee.		
145	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.		
146	Solution should monitor Non-financial transactions that include frequent PIN/ Password change in Cards/Internet Banking/Mobile Banking etc.		
147	Solution should monitor any additions, modifications, deletions to vital fields in Account, Customer Master files maintained in CBS system.		
148	Solution should monitor for events like frequent password resetting of the teller in Core Banking System.		
149	Solution should monitor for Customer Risk Profile changes from Higher to Lower classification.		

150	Solution should monitor Frequent locker operations (entries made in CBS).		
151	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.		
152	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.		
153	Solution should monitor for Issue of large number of cheque books in an account within a short time frame.		
154	Proposed solution should have the capability to detect anomalous customer behaviour or transactions originating from Omni channel.		
155	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.		
156	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.		
157	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).		
158	Proposed solution should have the ability to monitor all pre-login, login and post login transactions to detect any suspicious patterns.		
159	Proposed solution should provide pre-packaged scenarios to monitor pre-login, login and post login fraudulent patterns.		
160	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.		
161	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.		
162	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.		
163	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.		
164	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.		
165	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.		
166	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.		
167	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.		

168	Proposed system should ensure additional factor of authentication/ step up authenticationfor payment/login/non-financial events based on the policies.		
169	Proposed solution should be able to monitor the Fund transfers within own accounts, transfer to other accounts within the Bank.		
170	Proposed solution should be able to monitor the Standing Instruction set and Recurring transactions happening in Mobile and Internet.		
171	Proposed solution should be able to monitor the Fund transfers to other Bank accounts through Various modes like NEFT, RTGS, IMPS etc.		
172	Proposed solution should be able to monitor the Shopping/Bill Payment/Lifestyle events initiated from Omni Channel.		
173	Proposed solution should be able to configure policies based on non-financial events like Add Payee, Frequent Logins etc.		
174	Proposed solution offered should utilize device identification or machine fingerprinting.		
175	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.		
176	FRMS should have the ability to generate alerts in dormant accounts where there are unusual large transactions made through mobile application.		
177	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.		
178	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.		
179	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.		
180	Demonstration of ML models' ability to adapt and learn from new fraud patterns and data in real-time to continuously improve accuracy.		

181	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.		
182	Details on the vendor's XAI (Explainable AI) capabilities to ensure transparency in model decision- making for regulatory compliance and improved fraud analyst understanding.		
183	Vendor should be able to demonstrate tools and techniques for data preparation, feature engineering, and handling imbalanced datasets common in fraud data.		
184	Solution should use financial & non-financial transactions for behaviour profiling (scoring model).		
185	Solution should have ability to include different sets of limits and thresholds for different event types.		
186	Solution should provide bank with the capability to create, modify & delete models without any vendor dependency through GUI.		
187	There should be no restriction on the number of Models which can be deployed by the Bank.		
188	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.		
189	The solution should be able to compare between 2 or more existing models with the new model to understand the efficacy of the models.		
190	The solution to have a Self-Learning Risk Engine.		
191	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.		
192	Machine Learning proposed should be available at both macro level as well as hyper personalized level. ML models should continuously evolve		
193	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.		

194	Solution should update profiles in real time with every new transaction or event on the entity.		
195	The solution should have the capability to enrich data received from various data sources so that they can be used to profile the customer.		
196	Solution should be able to create scores that are portfolio specific and/ or relationship specific based on the profiles created.		
197	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.		
198	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.,		
199	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.		
200	The proposed solution should support building of scenarios across various banking channels like IMPS, UPI, Omni, RTGS, Debit Card, AEPS etc and there should be no restrictions in the no/type of channels used for framing policies. The proposed FRM Solution must carry out the monitoring across all transaction channels strictly based on Customer Identification Number (CIF no) only.		
201	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.		
202	Proposed Solution should allow business users to create their own dashboard and reports using a drag and drop graphical interface.		
203	Proposed Solution should allow end users to create custom reports using wide range of attributes including transaction attributes, case attributes, customer and account attributes.		
204	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.		

205	Proposed Solution should allow to export dashboard and reports to various formats including pdf, xls, html, Power BI etc.		
206	Proposed Solution should allow to configure these reports and dashboards to be sent to list of users via email.		
207	Proposed solution should allow complete slicing and dicing of reports and dashboards across various dimensions like product, channel, geography etc.		
208	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 FRMS or from external systems.		
209	Solution should visually prepare data for analysis, including joining tables, defining custom calculated columns and creating custom expressions for data tables available.		
210	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.		
211	The Solution should be able to generate periodic (Daily, Weekly, monthly etc.) customized reports to the Bank as per Bank's requirement.		
212	Solution should be able to Capture and report impact, loss averted, benefits realized.		
213	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.		
214	Solution should provide a summary report which summarizes the newly scheduled alert information to be made available to admin users.		
215	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 transactions).		
216	Proposed Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.		
217	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.		
218	The proposed solution should be able to combat both card present and card not present frauds in real-time.		
219	The solution should have capability to develop scenario and models related card transactions as per the need.		
220	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.		
221	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.		
222	Proposed Solution should support concept of dynamic and static daily limit for transactions to contain the risk in the event of card misuse.		
223	Proposed system should look for anomalous Card activity, It should detect behaviour associated with a fraudulent transaction.		
224	Solution should handle ISO 8583 based Advice message ((0120/220/420 message from Switch (ATM & AEPS)).		
225	Solution should handle ISO 8583 based Financial (0200)/400 / Authorization (0100) message from Switch (ATM & AEPS).		
226	Solution Should be able to detect the Nonfinancial transactions made through ATM which includes Balance enquiry ,Mini statement ,PIN change etc.		

227	Solution should be able to detect the POS Pre-auth, POS refund transactions.		
228	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.		
229	The solution should detect online banking sessions conducted from out-of-footprint geographies.		
230	The solution should identify transactions that are originated from high-risk internet vendors Domains, and flag sessions conducted from multiple locations in a short period of time.		
231	The Solution should alert on high velocity of pay-outs to multiple accounts through digital channels in short period of time in same day.		
232	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.		
233	Solution should monitor Average Daily/Weekly/Monthly FundsTransfer amount/ frequency by payee / biller and also preferred transaction hours for all channels.		
234	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.		
235	Solution should support various UPI transactions (P2P,P2M,M2P etc).		
236	Solution should be able to handle the financial and non-financial XML messages received in case of UPI & IMPS.		
237	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.		
238	Solution should be able to detect the new UPI registrations and provide the feedback to the system based on the customer profile.		
239	Solution should be able to accommodate rules based on the Location Information derived from AePS transactions.		

240	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.		
241	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.		
242	Solution should increase the risk score of the potential money mules and separate queue for these to be created in case management application.		
243	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.		
244	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.		
245	Solution should detect money mule accounts based on deviations from normal behaviour by using the statistical and machine learning techniques.		
246	Solution should be able to integrate to load data into an Operational Data Store and Data Lake as per the requirement of the Bank.		
247	Application should handle automatic switchover in cluster environment.		
248	Proposed Solution should have ability to failover without manual intervention.		
249	Proposed Solution Should be able to support different protocols (TCP/IP, IPX etc.). It should support IPV6.		
250	Proposed Solution should implement application patches and updates as specified in “Upgrades & Updates”, sub-section 3.1 above.		
251	Proposed Solution should support all the requirements mentioned in “Scope of Work” .		
252	System should track the client's IP, Network interface address and device.		

253	The solution should have the capability to support archiving the data on HDD/ Peripherals and retrieve from the above for the purpose of processing.		
254	Support for integration with packages like chart generators, Statistical/ Financial DLLs, MS Office Components, Power BI etc.		
255	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.		
256	Selected bidder should ensure that the solution is hardened as per the Secure Configuration provided by the Bank.		
257	Proposed solution should be able to cater to cloud data storage.		
258	Proposed solution should be compatible with Bank’s IPv4, IPv6 and TLS versions.		
259	The system should enable profiling of users and definition of control levels and passwords.		
260	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.		
261	System should provide auditable management of User-ids, access rights and passwords, login, activities etc.		
262	Maintenance of a secure, auditable log of access to the system, identifying user- Id, date, time, functions accessed, operations performed etc.		
263	Ensure data confidentiality and integrity at rest as well as in transit.		
264	Solution should support encryption as per industry standard encryption algorithms		

265	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.		
266	Daily activities log must be merged into the history log files.		
267	Enterprise Data Dictionary documents of the solution should be available.		
268	Service Lifecycle Management documents should be available.		
269	Date, time and User stamped process list for different processes.		
270	Provision for daily activity report/s to highlight all the processes invoked.		
271	Provision for recording of all unsuccessful login attempts.		
272	The solution should be Platform Agnostic and not be constrained to a single Hardware Platform/ Operating System/Database etc.		
273	The bidder to design the solution, security, and data flow architecture inline with the Bank's environment		
274	The bidder to develop, configure, customize, and implement the solution according to the project scope, technical specifications and functional specifications within the timelines		
275	Thebidder to ensure solution scalability and performance in line with Bank’s business projections and expected performance levels (SLAs)		
276	Testing of the proposed solution to also include Unit Testing, System Integration Testing, Performance Testing and Load Testing.		
277	Successful Bidder to fully support the UAT, security review, audits, or any other testing requirements of the Bank during the entire contract period		

278	Bidder to fix any vulnerabilities/bugs/issues in the platform at no additional cost		
279	Mustthe have capability to support Security mechanism such as TLS v1.2 and above, AD- Integration, Certificates and Key		
280	Secure exchange of payment messages not limited to secure message queues, secure file transfer, secure API.		
281	hash encrypted at storage over the network at least SHA1+Salt		
282	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.		
283	The Solution should support Anonymization (Removing PII) ,Pseudonymization (Replacing PII with artificial Identifiers) also Data minimization technique to be followed.		
284	Provide self-sufficient and easy access to enterprise data sources on multiple platforms, operating systems and databases.		
285	Display multiple results in one window to help better evaluate model performance.		
286	The proposed software must be able to accept text and should accept commonly used text sources such as ASCII text, document files, PDF files, spreadsheet files etc		
287	Should be capable of capturing feeds from multiple sources (like social media), analyse them and come up with insights. The analysis should be real time so as to ensure continuous tracking and detecting shifts in sentiment		
288	The solution should be available for real time (online) mode data quality implementation through a service oriented architecture		
289	The solution should have the capability to integrate the watch-list monitoring capabilities in real time		
290	FRMS must be monitored throughout 24x7 period, issuing appropriate alerts with system thresholds and heartbeats set correctly		

291	FRMS must be compliant with Information Security Policy		
292	FRMS must undergo full end to end testing including stress, performance, DR and recovery testing		
293	The system should have the ability to execute immediate card stops / temporary blocks/ Unblock the card		
294	The system should only be accessible by authorized Bank's users.		
295	The system should be configured with various user profiles with restricted privileges per user group depending on their role		
296	Ability for the fraud detection module to return with zero data loss to the last transaction handled in the event of a system recovery or restart, planned or unplanned,		
297	In case of a system failure, Ops risk, Payment Processing, Help Desk should be notified immediately.		
298	To facilitate real time alerts to customers on transactions (Fin & Non-Financial) system should have integration capabilities with Banks SMS and Email Gateway		
299	The proposed solution should be able to prevent existing and emerging frauds as result of phishing attacks, malware attacks, denial-of-service attack (Dos), Man-in-the-Middle (MITM) and Man-in-the-browser (MITB) attacks etc		
300	Ability to create Dashboard for top management with a drill down functionality		

Annexure 12-Service Level Agreement (SLA) & Penalties

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.

Uptime Percentage (A)	Penalty Details
A>=99.90%	No Penalty
99.89% => A> 99.5%	1% of cost of (Annual ATS charges)
99.5% => A > 98.5%	2% of cost of (Annual ATS charges)
A <= 98.5%	Penalty at an incremental rate of 1% (in addition to a base of 2%) of cost of (ATS) for every 0.1% lower than the stipulated uptime

In addition, the system has to respond back to source channel within maximum of 100 milliseconds on receipt of transaction from source channel at all times.

Response Time (A)	Penalty Details
A<=100 Milliseconds	No Penalty
A> 100 Milliseconds	If the number of transactions where the response time is greater than 100 milliseconds, is less than or equal to 10000 per day: 0.05% of cost of (Annual ATS charges). If the number of transactions where the response time is greater than 100 milliseconds, is greater than 10000 per day: 0.10 % of cost of (Annual ATS charges)

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 ATS payment.

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

Penalty on Account of delay during ATS

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 ATS cost per week of delay or part thereof subject to a maximum of 10% of the ATS for the total penalty levied in a single year.

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%.

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.

Penalty due to Audit and Compliance Gaps

Service	Gaps/Issue Categorization	Resolution Timelines	Penalty
AuditGaps/ Issues Resolution	Critical	Within 7 days	10,000 per day post resolution timelines till issues/gaps closure date.
	High	Within10 days	5,000 per day post resolution timelines till issues/gaps closure date.
	Medium	Within20 days	2,000 per day post the resolution timelines till the issues/gaps closure date.
	Low	Within 1 month	1,000 per day post the resolution timelines till the issues/gaps closure date.

Bidder must be submitting the compliance document confirming that the identified gaps have been closed.

Note:

If performance issues / downtime less than 98.00% 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. The maximum penalty amount cannot exceed the 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.

Monitoring and Audit

1. Compliance with security best practices may be monitored by periodic computer security audits / Information Security Audits performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audits may include, but are not limited to, a review of access and authorization procedures, backup and recovery procedures, network security controls and program change controls. The Vendor must provide the Bank access to various monitoring and performance measurement systems. The Vendor has to remedy all discrepancies observed by the auditors at no additional cost to the Bank.
2. For service level measurement, as defined in SLA, data recording is to be captured by the industry standard tools implemented by the Vendor. These tools should be a part of the proposed solution.

Annexure 13- Labour Law Compliance

To, Date

The Chief Operating Officer,

Head Office, Seven Oaks Building

Mallital, Nainital 263001

Dear Sir,

Sub: **Request for Proposal for Supply, Installation, Implementation, Integration, training & Maintenance of Fraud Risk Management System (FRM) Solution in the Bank**

Ref: Your RFP No. **NTB/IT/FRMS/2025/03/023 dated 21/03/2025**

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 14 - Reference Site Details

The reference sites submitted must be necessarily of those Banks/Companies where the bidder has been awarded the contract prior to date of issuance of this RFP and implemented in steady state not for where the offered solution is accepted but implementation is not completed. Please provide reference details in the format defined below:

Sr No	Name of Implementation/Client	
1	Successful establishment of FRMS for Bank. The following may be given Bank wise: ➢ 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	
	➢ 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 The Nainital Bank Limited can contact reference site to seek further information.	

(Enclose necessary documentary proof)

Place:
Date:
Signature Name & Designation:
Business Address:

Annexure 15- Commercial Bid Format

SL. No.	Items	OTC (One Time Cost)	YEARLY	TOTAL
			AMT	AMT
1	License Cost	0.00	X	0.00
2	Implementation Cost	0.00	X	0.00
3	ATS (Annual Technical Support)	X	0.00	0.00
4	Onsite Support Charges	X	0.00	0.00
5	AnyOther Charges **	0.00	0.00	0.00
Total				**0.00**

Note

a. For each of the above items provided the bidder is required to provide the cost for every line item where the bidder has considered the cost in BOM.

b. The bidder needs to clearly indicate if there are any recurring costs included in the above bid and quantify the same. In the absence of this, the bidder would need to provide the same without any charge. Bidder should make no changes to the quantity.

c. 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.

d. All Deliverables to be supplied as per RFP requirements provided in the tender

e. The Service Charges need to include all services and other requirement as mentioned in the RFP

f. The bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations.

g. The prices quoted by the bidder shall be all inclusive, that is, inclusive of all taxes, duties, levies etc. except GST. ** Details to be provided for any commercial provided against “Any Other Charges”.

h. Onsite Support for the solution will be 24x7 and charges to be provided based on the manpower efforts in 3 shifts per day. The Bank has discretion to avail onsite support services and number of support engineers at person day cost given. However, for the TCO purpose 3-person day (3 shift x 1 person) x 365 for each year will be considered

Authorized Signatory Name:
Designation:

Bidder’s Corporate Name

Annexure 16- Integrity Pact

PRE CONTRACT INTEGRITY PACT

(TO BE STAMPED AS AN AGREEMENT AS APPLICABLE TO THE STATE OF UTTARAKHAND)

THE NAINITAL BANK LIMITED, a Scheduled Commercial bank incorporated under the Companies Act, 1956 (now the Companies Act, 2013) having its Registered Office at G.B. Pant Road, Nainital and its Head Office at Seven Oaks Building, Mallital, Nainital (CIN No. U65923UR1922PLC000234) (hereinafter referred to as the "Bank" which expression shall mean and include its Administrator, legal representatives, successors-in-interest, Executors and permitted assigns) and represented herein by its authorized signatory;

And

_____, a company incorporated under the (Indian) Companies Act, _____ and whose registered office is at _____ _____ through its authorized representative Mr._____ _____ hereinafter referred to as "Bidder", which expression shall, unless it be repugnant to the meaning or context thereof, be deemed to mean and include its successors and permitted assigns)

Preamble

The Nainital Bank Ltd. is a Scheduled Commercial Bank having its presence across five states i.e. Uttarakhand, Uttar Pradesh, Delhi, Haryana and Rajasthan. The Nainital Bank Ltd. is committed to fair and transparent procedures in appointing of its outsource vendors.
The Nainital Bank Ltd. intends to select bidder, under laid down organizational procedures, contract/s for Supply, Implementation & Maintenance of Fraud Risk Management System.
The Nainital Bank Ltd. 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).

Section 1 - Commitments of The Nainital Bank Ltd.

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

   a. No employee of the The Nainital Bank Ltd., personally or through its family members, will in connection with the RFP for, or the execution of a contract, demand; take a promise for or accept, for self or third person, any monetary or non-monetary benefit which the person is not legally entitled to.

   b. The Nainital Bank Ltd. will, during the RFP process treat all Bidder(s) with equity and reason. The Nainital Bank Ltd. will in particular, before and during the RFP 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 RFP process or the contract execution.

   c. The Nainital Bank Ltd. will make endeavour to exclude from the selection process all known prejudiced persons.

2. If The Nainital Bank Ltd. 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 Nainital Bank Ltd. will inform the Bank's Chief of Internal Vigilance and in addition can initiate disciplinary actions.

Section 2 - Commitments of the Bidder(s)/ Contractor(s)

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

   a. The Bidder(s) / Contractor(s) will not, directly or through any other person or firm, offer, promise or give to any of the employees of The Nainital Bank Ltd. involved in the RFP 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 RFP process or during the execution of the contract.

   b. 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.

   c. 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 purposes of competition or personal gain, or pass on to others, any information or document provided by The Nainital Bank Ltd. as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

   d. The Bidder(s) / Contractors(s) of foreign origin shall disclose the name and address of the Agents/ representatives in India, if any, similarly the Bidder(s) / Contractors(s) of Indian Nationality shall furnish the name and address of the foreign principals, if any.

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

   f. Bidder(s) / Contractor(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to the Bank's Chief of Internal Vigilance and shall wait for their decision in the matter.

   g. 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 RFP process and exclusion from future contracts

If the Bidder(s) /Contractor(s), before empanelment or during empanelment has committed a transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, The Nainital Bank Ltd. is entitled to disqualify the Bidder(s) / Contractor(s) from the RFP process or take action as per law in force.

Section 4 - Compensation for Damages

1. If The Nainital Bank Ltd. has disqualified the Bidder(s) from the RFP process prior to the award according to Section 3, The Nainital Bank Ltd. is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security.

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

Section 5 - Previous transgression

1. The Bidder 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 Public Sector Enterprise in India, that could justify his exclusion from the RFP process.

2. If the Bidder makes incorrect statement on this subject, he can be disqualified from the RFP process

Section 6 - Equal treatment of all Bidders | Contractors | Subcontractors

1. In case of Sub-contracting, the Principal Contractor shall take the responsibility of the adoption of Integrity Pact by the Sub-contractor.

2. The Nainital Bank Ltd. will enter into agreements with identical conditions as this one with all Bidders and Contractors.

3. The Nainital Bank Ltd. will disqualify from the RFP process all bidders who do not sign this Pact or violate its provisions.

Section 7 - Criminal charges against violating Bidder(s) | Contractor(s) | Subcontractor(s)

If The Nainital Bank Ltd. obtains knowledge of the conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if The Nainital Bank Ltd. has substantive suspicion in this regard, The Nainital Bank Ltd. will inform the same to the Bank's Chief of Internal Vigilance.

Section 8 - Pact Duration

This Pact shall be effective from the date of its execution, and shall expire for the selected Contractor till the contract period, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the bidders and exclusion from future business dealings.

Section 10. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission,

The Nainital Bank Ltd. or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

Section 11 - Other provisions

1. This agreement is subject to Indian Law and court at Nainital shall have exclusive jurisdiction to entertain any matter arising out of this pact.

2. Changes and supplements as well as termination notices need to be made in writing.

3. If the Contractor is a partnership or a consortium, this agreement must be signed by all partners or consortium members.

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

5. Issues like scope of work, Warranty / Guarantee etc. shall be outside the purview of the Bank's Chief of Internal Vigilance.

6. In the event of any contradiction between the Integrity Pact and RFP/ RFQ/ RFP documents and its Annexure, the Clause in the Integrity Pact will prevail.

The parties hereby sign this Integrity Pact at _____ on_____

THE NAINITAL BANK LTD.
Name of the Officer:
Designation:
Date:
Place:
Witness
1. _____
2. _____

BIDDER
Chief Executive Officer
Department:
Date:
Place:
Witness
1. _____
2. _____

--End of Document---

Annexure 17 Executive Summary (To be submitted as part of Eligibility Bid)

Executive Summary:

- The Executive Summary should be limited to a maximum of five pages and should summarize the content of the response. The Executive Summary should initially provide

  i) An overview of Vendor's organization and position with regards to providing Fraud Risk Management System

  ii) A summary of the Vendor's services related to the proposal that will be provided as a part of this procurement

  iii) Brief description of the unique qualifications of the Vendor

  iv) A summary on capabilities such as resources and past experience of providing such solution

Annexure 18 Executive Technical Summary (To be submitted as part of Technical Bid)

Executive Technical Summary:

- The Executive Summary should be limited to a maximum of five pages and should summarize the content of the response. The Executive Summary should initially provide

i) An overview of Vendor's organization and position with regards to providing Fraud Risk Management System

ii) A summary of the Vendor's services related to the proposal that will be provided as a part of this procurement

iii) Brief description of the unique qualifications of the Vendor

iv) A summary on capabilities such as resources and past experience of providing such solution

v) Response to the technical requirements in Annexure 11 explaining the technical specifications wherever required. Information provided in the Executive Summary is to be presented in a clear and concise manner.

- Technical Proposal: The proposal based on Technical requirement as per **Annexure 11** should be submitted with pages properly numbered, each page signed and stamped. The Technical Proposal should be bound in such a way that the sections of the Proposal cannot be removed and separated easily.